Textos Universitários

Jamil Ferreira

A Construção dos Números

Sumário

1

Preliminares

1.1 Notas históricas

"A matemática partia de verdades evidentes e prosseguia através de raciocínios cuidadosos para descobrir verdades escondidas" ([6], p. 306).

A matemática sempre representou uma atividade humana e, em todas as épocas, mesmo nas mais remotas, a ideia de contar sempre esteve presente. Um clássico exemplo da noção intuitiva de contagem era a correspondência entre ovelhas de um rebanho e pedrinhas contidas em pequenos sacos, ou marcas em pedaço de osso ou de madeira, ou ainda através de nós em cordões, utilizados pelos incas.

Muitos anos ainda se passaram até que se iniciasse o desenvolvimento teórico do conceito de número que, embora hoje nos pareça natural, foi lento e complexo, envolvendo diversas civilizações.

Os registros históricos nos mostram a utilização de vários sistemas de numeração, por exemplo, os povos babilônios de 2000 a.C., que desenvolveram o sistema

de numeração sexagesimal e empregaram o princípio posicional; os egípcios, que já usavam sistema decimal (não posicional); os romanos, que fizeram história através do uso simultâneo do princípio da adição e do raro emprego do princípio da subtração; e os gregos antigos, povos que utilizavam diversos sistemas de numeração.

Quase quatro mil anos separam as primeiras manifestações de numeração escrita da construção do sistema de numeração posicional decimal que utilizamos, munido do símbolo denominado zero. Esse símbolo foi criado pelos hindus nos primeiros séculos da era cristã. A concepção do zero foi ignorada, durante milênios, por civilizações matematicamente importantes como a dos gregos e dos egípcios.

A invenção do zero foi um passo decisivo para a consolidação do sistema de numeração indo-arábico, devido à sua eficiência e funcionalidade em relação aos demais sistemas de numeração. Como efetuaríamos, por exemplo, a multiplicação 385×9.807 usando algarismos romanos?

A heterogeneidade de técnicas utilizadas nas representações numéricas não impediu, no entanto, que os cientistas da antiguidade pensassem em questões profundas e essenciais da matemática.

Um marco importante na história dos números e da matemática se deu no século VI a.C., na Escola Pitagórica. Em seus estudos, os pitagóricos envolviam-se de um certo misticismo, pois acreditavam que existia uma harmonia interna no mundo, governada pelos números naturais.

Desde Pitágoras, pensava-se que, dados dois segmentos de reta quaisquer, AB e CD, seria sempre possível encontrar um terceiro segmento EF, contido um número inteiro de vezes em AB e um número inteiro de vezes em CD. Expressamos essa situação dizendo que EF é um *submúltiplo comum* de AB e CD ou que AB e

CD são *comensuráveis*.

Essa ideia nos permite comparar dois segmentos de reta da seguinte maneira: dados dois segmentos, AB e CD, dizer que a razão AB/CD é o número racional m/n, significa que existe um terceiro segmento EF, submúltiplo comum desses dois, satisfazendo: AB é m vezes EF e CD é n vezes EF.

É natural imaginarmos que, para dois segmentos AB e CD dados, é sempre possível tomar EF suficientemente pequeno para caber um número inteiro de vezes simultaneamente em AB e em CD. Em outras palavras, que dois segmentos de reta são sempre comensuráveis, como pensavam os pitagóricos, sendo, portanto, os números naturais suficientes para expressar a razão entre eles e, de modo mais geral, a relação entre grandezas da mesma natureza.

O reinado dos números naturais, na concepção pitagórica, foi profundamente abalado por uma descoberta originada no seio da própria comunidade pitagórica e que se deu, em particular, numa figura geométrica comum e de propriedades aparentemente simples, o quadrado. Trata-se da *incomensurabilidade* entre a diagonal e o lado de um quadrado.

De fato, ao considerarmos a diagonal e o lado de um quadrado comensuráveis, teremos, digamos, a diagonal com medida nt e o lado com medida mt. Segue-se, pelo Teorema de Pitágoras, que:

$$n^2t^2 = m^2t^2 + m^2t^2 \Rightarrow n^2t^2 = 2m^2t^2 \Rightarrow n^2 = 2m^2,$$

o que é absurdo, pois em n^2 há uma quantidade par de fatores primos e, em $2m^2$, uma quantidade ímpar de fatores primos, em contradição com a unicidade da decomposição de um número natural em fatores primos, como mostra o Teorema Fundamental da Aritmética. (Esse teorema, que usamos desde o ensino básico de matemática,

está exposto rigorosamente em vários itens da bibliografia, por exemplo, em [5], [14], [18], [25] e [31].)

Essa situação só foi contornada através do matemático e astrônomo ligado à Escola de Platão, Eudoxo de Cnidos (408 a.C. – 355 a.C.), que criou a *Teoria das Proporções* para tratar as grandezas incomensuráveis através da geometria (veja [1]), o que, embora genial, contribuiu para a desaceleração do desenvolvimento da aritmética e da álgebra por muitos séculos.

O coroamento da fundamentação matemática do conceito de número ocorreu somente no final do século XIX, principalmente através dos trabalhos propostos por Richard Dedekind (1831-1916), Georg Cantor (1845-1918) e Giuseppe Peano (1858-1932). Esses estudos foram motivados pelas demandas teóricas que surgiram a partir do volume de conhecimento matemático adquirido a partir do cálculo diferencial e integral de Isaac Newton (1643-1727) e Gottfried Leibniz (1646-1716), no século XVII.

É interessante notar como o processo histórico da conceituação de número assemelha-se à nossa própria formação desse conceito. Desde crianças, admitimos os números naturais como fruto do processo de contagem, da mesma forma que a humanidade os admitiu até o século XIX. Aliás, entre os gregos da época de Euclides, números eram os que hoje escrevemos como 2, 3, 4, 5 etc., ou seja, os naturais maiores do que 1. O próprio 1 era concebido como a unidade básica a partir da qual os números, as quantidades, eram formadas. O zero, como vimos, foi uma concepção já dos primeiros séculos da era cristã, criada pelos hindus, para a numeração escrita. Para uma criança aprendendo a contar, este ato só faz sentido a partir da quantidade 2, senão, contar o quê? Ela só admite o zero depois de ter

passado alguns anos experimentando os números "de verdade", isto é, contando e adquirindo experiência, o que se dá no início de sua aprendizagem da numeração escrita.

As frações eram admitidas pelos gregos não como números, mas como razão entre números $(1, 2, 3, 4$ etc.). Da mesma forma, os números negativos, inicialmente utilizados para expressar dívidas, débitos e grandezas que são passíveis de serem medidas em sentidos opostos, só receberam o *status* de números séculos após serem utilizados na matemática e em suas aplicações. Novamente podemos observar a semelhança com a nossa experiência pessoal em matemática.

A existência de grandezas incomensuráveis e a ausência de um tratamento eficiente para expressá-las, isto é, o desconhecimento de uma fundamentação teórica para o conceito de número real, não impediu o progresso de ramos da matemática do século XVI ao século XIX. No entanto, a complexidade dessa matemática conduziu a problemas para cuja compreensão e solução o entendimento intuitivo não era suficiente. É mais ou menos assim que formamos o nosso conceito de número real: apesar de ouvirmos falar de números reais desde o Ensino Fundamental, concretamente só trabalhamos com números racionais naquela fase ou, no máximo, manipulamos números que aprendemos a chamar de "reais". Isso ocorre até no Ensino Superior e, mais grave, em não raras faculdades de matemática, os formandos concluem o seu curso com a mesma ideia de número real com que nele ingressaram.

Os números complexos apareceram no estudo de equações, no século XVI, com o matemático italiano Girolamo Cardano (1501-1576), mas também só adquiriram o *status* de número a partir de suas representações geométricas, dadas no século XVIII (por K. F. Gauss (1777-1855) e J. R. Argand (1768-1822)), e da sua estrutura

algébrica, apresentada por W. R. Hamilton em 1833, na qual eles eram definidos como pares ordenados de números reais. Estes, por sua vez, foram construídos rigorosamente a partir dos racionais, décadas depois, por R. Dedekind e G. Cantor. Aqui também há um paralelo com a nossa educação escolar: supondo conhecidos os reais, não é tão complicado concebermos os complexos. No entanto, o conceito rigoroso de número real só se aborda num primeiro curso de análise matemática na universidade. Isso, porém, costuma ser feito de forma axiomática, isto é, o conjunto dos números reais é admitido por axioma como um corpo ordenado completo, e não construído a partir dos racionais, como faremos neste livro, adaptando o trabalho de Dedekind.

Por fim, os números racionais podem ser construídos rigorosamente a partir dos números inteiros e esses a partir dos naturais. Mas, e os números naturais, os primeiros que são admitidos pela nossa intuição? Assim se perguntaram alguns matemáticos do século XIX, na busca de completar o conceito matematicamente rigoroso de número. Eles podem ser construídos a partir da Teoria dos Conjuntos (veja [17], [30]) ou podem ser apresentados através de axiomas, como fez G. Peano, em 1889, e como faremos aqui, com as devidas adaptações. Observe que aqui também continua o paralelo com a nossa formação matemática escolar, uma vez que o questionamento sobre a natureza dos números naturais é inexistente para a quase totalidade das pessoas que não são diretamente envolvidas com matemática.

Assim, a apresentação que faremos nos capítulos seguintes é aquela que os matemáticos do século XIX e XX deixaram pronta para nós, possibilitando-nos apresentar os conjuntos numéricos numa ordem logicamente coerente, rápida e elegante - naturais, inteiros, racionais, reais e complexos - passando a limpo a conflituosa

ordem histórica delineada acima.

A citação abaixo ilustra bem o movimento pelos fundamentos da matemática que acabamos de comentar:

> *Além da libertação da geometria e da libertação da álgebra, um terceiro movimento matemático profundamente significativo teve lugar no século XIX. Esse terceiro movimento, que se materializou lentamente, tornou-se conhecido como aritmetização da análise. ([10], p. 609).*

1.2 Relações de equivalência

O conceito de relação de equivalência permeia grande parte deste livro. Por isso, trataremos dessa questão a partir de agora.

Admitiremos a noção intuitiva de conjuntos e, em particular nesta seção, dos conjuntos numéricos e das propriedades básicas de suas operações. Não esqueçamos que nosso objetivo nos capítulos seguintes é estudar o conceito rigoroso de número, portanto desses conjuntos numéricos.

Utilizaremos a notação usual para os conjuntos numéricos:
$\mathbb{N} = \{0, 1, 2, \ldots\}$ que é o conjunto dos números naturais, $\mathbb{Z}$ (conjunto dos números inteiros), $\mathbb{Q}$ (conjunto dos números racionais), $\mathbb{R}$ (conjunto dos números reais) e $\mathbb{C}$ (conjunto dos números complexos). Se A é subconjunto de $\mathbb{R}$, A_+ denota o conjunto dos elementos não negativos de A e A_- o dos elementos não positivos. Se B é um conjunto de números que contém o zero, então B^* denota $B \setminus \{0\}$. (O símbolo "$\setminus$" denota aqui diferença de conjuntos.)

Definição 1.2.1. Seja A um conjunto. O *conjunto das partes de* A, ou *conjunto potência de* A, denotado por $\mathcal{P}(A)$, é o conjunto cujos elementos são os subconjuntos de A.

Exemplo 1.2.1.

1. Se $A = \{a,b\}$, então $\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, A\}$.
2. Se $A = \emptyset$, então $\mathcal{P}(A) = \{\emptyset\}$, pois $\emptyset$ é o único subconjunto de A.

Exercício 1. Descreva $\mathcal{P}(A)$ nos seguintes casos:

1. $A = \{1,2,3\}$;
2. $A = \{\emptyset\}$;
3. $A = \{1,2,3,\ldots\}$;
4. $A = \mathcal{P}(\{1,2\})$;
5. $A = \mathcal{P}(B)$, onde $B = \mathcal{P}(\{1\})$.

Definição 1.2.2. Dados um conjunto não vazio A e $a,b \in A$, definimos o *par ordenado* (a,b) como sendo o conjunto $\{\{a\},\{a,b\}\}$ (observe que $(a,b) \subset \mathcal{P}(A)$).

Esta definição tem por objetivo tornar preciso matematicamente o conceito de par ordenado que, desde o Ensino Fundamental, admitimos intuitivamente como "um par de objetos onde a ordem tem importância".

Com a definição acima, mostramos, no teorema seguinte, que par ordenado é aquilo que concebíamos intuitivamente.

Teorema 1.2.1. *Sejam A um conjunto e $a,b,c,d \in A$. Temos que:*

$$(a,b) = (c,d) \Leftrightarrow a = c \;\; e \;\; b = d.$$

Demonstração. Se $a = c$ e $b = d$, então é claro que $(a,b) = (c,d)$. Reciprocamente, suponhamos que $(a,b) = (c,d)$, isto é, que $\{\{a\},\{a,b\}\} = \{\{c\},\{c,d\}\}$. Consideremos dois casos:

1º caso: $a = b$.

Nesta situação, $(a,b) = (a,a) = \{\{a\},\{a,a\}\} = \{\{a\},\{a\}\} = \{\{a\}\}$. Assim, nossa hipótese fica $\{\{a\}\} = \{\{c\},\{c,d\}\}$. Então o conjunto $\{c,d\}$ é um elemento de $\{\{a\}\}$, logo só pode ser igual a $\{a\}$, o que acarreta $c = d = a$. Como $a = b$, obtemos $a = c$ e $b = d$ (todos iguais a a).

2º caso: $a \neq b$.

Analisemos então a igualdade $\{\{a\},\{a,b\}\} = \{\{c\},\{c,d\}\}$:

Se fosse $\{a,b\} = \{c\}$, teríamos $a = b = c$, contradizendo a hipótese $a \neq b$. Logo $\{a,b\} = \{c,d\}$, de onde pode-se concluir que $c \neq d$. Daí, o elemento $\{a\}$ não pode ser $\{c,d\}$, logo $\{a\} = \{c\}$, de onde obtemos que $a = c$. De $\{a,b\} = \{c,d\}$, como $b \neq a = c \neq d$, segue que $b = d$. □

Definição 1.2.3. Dado um conjunto A, o *produto cartesiano de A por A*, denotado por $A \times A$, é o conjunto de todos os pares ordenados compostos por elementos de A, isto é, $A \times A = \{(x,y) \mid x,y \in A\}$.

Exemplo 1.2.2.

1. Se $A = \{1,2\}$, então $A \times A = \{(1,1),(1,2),(2,1),(2,2)\}$.

2. Se $A = \emptyset$, então $A \times A = \emptyset$.

Exercício 2. Se $A = \{1,2,3\}$, quantos elementos possui $A \times A$? Generalize.

Definição 1.2.4. Dados dois conjuntos A e B, se $x \in A$ e $y \in B$ então $x, y \in A \cup B$, e podemos considerar (x,y) como na Definição 1.2.2, isto é, $(x,y) = \{\{x\},\{x,y\}\} \subset \mathcal{P}(A \cup B)$. Definimos o *produto cartesiano de A por B* como sendo o conjunto $A \times B = \{(x,y) | \, x \in A \text{ e } y \in B\}$.

Observe que $A \times B \subset \mathcal{P}(\mathcal{P}(A \cup B))$ (certifique-se deste fato).

Exercício 3. $A \times B$ é igual a $B \times A$? Justifique.

Exercício 4. Mostre que se A ou B for o conjunto vazio, então $A \times B = \emptyset$.

Exercício 5. Dados três elementos a, b e c, pertencentes, respectivamente, aos conjuntos A, B e C, definimos a *terna ordenada* (a,b,c) como sendo o par ordenado $((a,b),c)$ pertencente a $(A \times B) \times C$.

1. Mostre que $(a,b,c) = (x,y,z)$ se, e somente se, $a = x$, $b = y$ e $c = z$.

2. Como você definiria o produto cartesiano de três conjuntos A, B e C?

3. Como você definiria uma quádrupla ordenada de elementos de um conjunto A? E o produto cartesiano de quatro conjuntos?

4. Generalize.

Exercício 6. Uma *operação* em um conjunto não vazio A é uma função $* : A \times A \to A$. A imagem $*((x,y))$ de um par ordenado (x,y) pela função $*$ é usualmente denotada por $x * y$. Considerando o nosso conceito intuitivo de conjuntos numéricos e de suas "operações aritméticas", pergunta-se: quais das quatro

"operações aritméticas fundamentais" são de fato operações, no sentido da definição acima, no conjunto dos números naturais? E no conjunto dos inteiros? Mesma pergunta para os racionais, reais e complexos.

Definição 1.2.5. Uma *relação binária* R num conjunto A é qualquer subconjunto do produto cartesiano $A \times A$, isto é, $R \subset A \times A$.

Exemplo 1.2.3. Se $A = \{1,2,3\}$, então $R = \{(1,1),(1,2),(1,3),(3,1),(3,3)\}$ é uma relação binária em A.

Notação: Se R é uma relação binária em A e se $(a,b) \in R$, escrevemos aRb, isto é, $(a,b) \in R \Leftrightarrow aRb$. Lê-se: a está relacionado com b (via R). Assim, no exemplo acima, temos, por exemplo, $1R2$, mas não temos $2R1$.

Uma relação binária em A será chamada simplesmente de *relação em A*, pois não trataremos de relações que não sejam binárias.

Definição 1.2.6. Uma relação R em A diz-se *relação de equivalência* se possuir as seguintes propriedades:

i) *reflexiva*: aRa, para todo $a \in A$;

ii) *simétrica*: se $a,b \in A$ e aRb, então bRa;

iii) *transitiva*: para $a,b,c \in A$, se aRb e bRc, então aRc.

Exemplo 1.2.4. A relação R do exemplo anterior não é reflexiva nem simétrica, mas é transitiva (verifique). Logo, R não é relação de equivalência.

Exemplo 1.2.5. Consideremos o conjunto $A = \{a,b,c\}$. Verifiquemos se as relações abaixo são relações de equivalência no conjunto A:

1. $R = \{(a,a),(a,b),(b,c),(a,c),(b,a)\}$;

2. $S = \{(a,a),(b,b),(c,c),(a,b),(b,a)\}$.

Temos:

1. R não é uma relação de equivalência, pois não é reflexiva: $(b,b) \notin R$. Observe que (c,c) também não está em R e que R também não é simétrica e nem transitiva (verifique!).

2. S é uma relação de equivalência (verifique!).

No início desta seção, dissemos que admitiríamos nela a noção intuitiva dos conjuntos numéricos e de suas propriedades aritméticas básicas. Ela será necessária no exemplo seguinte e em algumas outras poucas situações desta seção. O leitor não precisa incomodar-se com essa utilização, porque ela se dará apenas a título de esclarecer o conceito de relação de equivalência, este, sim, rigorosamente tratado na presente seção. Além disso, nada do que dissermos sobre esses conjuntos aqui servirá de base para as construções rigorosas deles, que são objeto dos capítulos seguintes.

Exemplo 1.2.6. Se $a,b \in \mathbb{Z}$, dizemos que *a divide b* (ou *b* é *múltiplo de a*, ou *a* é *divisor de b*) se existir $c \in \mathbb{Z}$ tal que $b = ac$. Escrevemos $a \mid b$ para simbolizar que a divide b. Esta relação de divisibilidade em $\mathbb{Z}$ não é uma relação de equivalência, porque não é simétrica, apesar de ser reflexiva e transitiva (verifique!).

Se R é uma relação de equivalência e aRb, dizemos que a é *R-equivalente* a b ou, simplesmente, a é *equivalente* a b, quando R estiver subentendida no contexto.

Exercício 7. Seja A um conjunto. Mostre que:

1. $A \times A$ é uma relação de equivalência em A.

2. $\{(x,x) \mid x \in A\}$ é uma relação de equivalência em A. Esta relação se chama *igualdade em A* (ou *identidade de A*), e se denota por "$=$". Logo $(x,x) \in =$, $\forall x \in A$, que escrevemos usualmente como $x = x$, $\forall x \in A$.

3. Qualquer relação de equivalência em A está compreendida entre as duas dos itens anteriores.

Definição 1.2.7. Sejam R uma relação de equivalência num conjunto A e $a \in A$ um elemento fixado arbitrariamente. O conjunto

$$\overline{a} = \{x \in A \mid xRa\}$$

chama-se *classe de equivalência de a pela relação R*. Ou seja, $\overline{a}$ é o conjunto constituído por todos os elementos de A que são equivalentes a a.

Exemplo 1.2.7. As classes de equivalência dadas pela relação S do Exemplo 1.2.5 são $\overline{a} = \{a,b\}$, $\overline{b} = \{b,a\}$, e $\overline{c} = \{c\}$.

Teorema 1.2.2. *Sejam R uma relação de equivalência em um conjunto A e a e b elementos quaisquer de A, então:*

i) $a \in \overline{a}$;

ii) $\overline{a} = \overline{b} \Leftrightarrow aRb$;

iii) $\overline{a} \neq \overline{b} \Rightarrow \overline{a} \cap \overline{b} = \emptyset$.

Demonstração. (i) e (ii) ficam a cargo do leitor como exercício. Mostremos (iii) por contraposição. Suponhamos então que exista $c \in \overline{a} \cap \overline{b}$. Então, aRc e cRb. Pela transitividade, aRb e, consequentemente, por (ii), segue que $\overline{a} = \overline{b}$, contrariando a hipótese. □

A propriedade (iii) acima nos mostra que duas classes de equivalência distintas são disjuntas.

Uma conclusão importante do item (ii) desse Teorema 1.2.2 é que, dado um elemento arbitrário x da classe de equivalência $\overline{a}$, então $\overline{x} = \overline{a}$, isto é, todo elemento de uma classe de equivalência $\overline{a}$ tem a mesma classe de equivalência de a. Dizemos então que $\overline{a}$ pode ser representada por $\overline{x}$, $\forall x \in \overline{a}$ (ou, ainda, que x é um representante de $\overline{a}$, $\forall x \in \overline{a}$).

Exemplo 1.2.8. Sejam $A = \mathbb{Z}$ e R a relação dada por: aRb quando o resto das divisões de a e de b por 2 forem iguais. Por exemplo, $(5,21) \in R$, $(6,14) \in R$, mas $(5,8) \notin R$. Verifique como exercício que R é uma relação de equivalência em $\mathbb{Z}$. Com isso:

$$\overline{1} = \{\ldots,-3,-1,1,3,5,\ldots\} = \overline{3} = \overline{5} = \overline{-7},\ldots$$
$$\overline{2} = \{\ldots,-4,-2,0,2,4,\ldots\} = \overline{0} = \overline{-2} = \overline{6}\ldots$$

Verifique que só há duas classes de equivalência distintas. Mais precisamente, tem-se $\overline{n} = \overline{0}$ para n par e $\overline{n} = \overline{1}$ para n ímpar.

Definição 1.2.8. Seja R uma relação de equivalência num conjunto A. O conjunto constituído das classes de equivalência em A pela relação R é denotado por A/R e denominado *conjunto quociente* de A por R.

Assim, $A/R = \{\overline{a} \,|\, a \in A\}$.

Exemplo 1.2.9. Se R é a relação do exemplo anterior, então $A/R = \{\overline{0}, \overline{1}\}$.

Exercício 8. Seja $A = \{1,2,3\}$. Determine os elementos de $A/(A \times A)$ e $A/=$.

Exercício 9. Considere a seguinte relação $\sim$ em $\mathbb{Z}$: $x \sim y$ quando os restos das divisões de x e y por 3 forem iguais.

1. Mostre que $\sim$ é relação de equivalência em $\mathbb{Z}$.

2. Encontre $\mathbb{Z}/\sim$.

3. Generalize este exercício e o Exemplo 1.2.8.

Exercício 10. Seja A o conjunto de todas as pessoas e R a relação em A dada por xRy quando x for mãe de y.

1. R é relação de equivalência?

2. Na sua casa há pessoas para comporem elementos de R? Em caso positivo, descreva esses elementos.

Exercício 11. Seja A como no Exercício 10 e S a relação em A dada por xSy quando x for irmão (irmã) de y ou quando x e y forem a mesma pessoa. (Nesses tempos modernos, convém definir, neste contexto restrito, o termo "irmão": x e y são irmãos quando são filhos biológicos do mesmo pai e da mesma mãe.) Mostre que S é uma relação de equivalência. Qual é a classe de equivalência cujo representante é você? Na sua casa há pessoas para comporem elementos de S? Em caso positivo, descreva esses elementos. Qual a classe de equivalência de cada pessoa que mora em sua casa? O que ocorreria se a definição de S fosse simplesmente "xSy quando x for irmão (irmã) de y"?

Exercício 12. Seja A um conjunto e $A = A_1 \cup A_2 \cup A_3 \ldots \cup A_n$ uma *partição finita de* A, isto é, uma decomposição de A como união finita de uma família de subconjuntos de A que são dois a dois disjuntos e não vazios. Para x e $y \in A$, definimos a seguinte relação R: xRy quando x e y pertencem ao mesmo elemento da partição. Em símbolos: $xRy \Leftrightarrow$ existe $i \in \{1, \ldots, n\}$ tal que $x, y \in A_i$. Mostre que R é uma relação de equivalência em A.

Mesmo que a partição de A consista de uma família infinita de subconjuntos de A, a relação R do exercício acima ainda é de equivalência.

Observe que uma relação de equivalência R em A determina uma partição de A, a saber, as classes de equivalência determinadas por R. Reciprocamente, vimos acima que uma partição qualquer de A determina uma relação de equivalência em A. Além disso, as classes de equivalência dessa relação são precisamente os subconjuntos que compõem a partição. Confira!

Exercício 13. Seja $A = A_1 \cup A_2$ tal que $A_1 \cap A_2 \neq \emptyset$. Definindo a relação R em A como no exercício anterior, ela é relação de equivalência?

Exercício 14. Explicite todas as relações de equivalência no conjunto $A = \{1,2,3\}$.

Exercício 15. Seja $A = \{x \in \mathbb{Z} | -5 \leq x \leq 10\}$. Sejam R, S, T e U as relações sobre A definidas por:

$xRy \Leftrightarrow x^2 = y^2$;

$xSy \Leftrightarrow$ existe $k \in \mathbb{N}$ tal que $x^2 = y^2 + k$;

$xTy \Leftrightarrow$ existe $k \in \mathbb{Z}$ tal que $x^2 = y^2 + k$;

$xUy \Leftrightarrow$ existe $k \in \mathbb{Z}$ tal que $x - y - 3k = 0$.

Verifique que R, T e U são relações de equivalência, mas S não o é. Determine os respectivos conjuntos quocientes: A/R, A/T e A/U.

2

Números naturais

A ideia de número natural sempre esteve associada à ideia de quantidade e à necessidade de contagem. A formalização do conceito de número natural como expressão de quantidade se dá através da Teoria dos Conjuntos. Uma referência clássica para a construção dos números naturais via Teoria dos Conjuntos é [17]. Veja também [30].

Uma outra opção de formalização, que adotaremos aqui, é a axiomática, não construtiva. Ela consiste simplesmente em assumir a existência do conjunto dos números naturais (a partir do qual *construiremos* os demais conjuntos numéricos). Mas o que significa "assumir a existência do conjunto dos números naturais"? Significa assumir a existência de um conjunto satisfazendo certos axiomas que são capazes de caracterizar completamente, e de forma rigorosa, a nossa ideia intuitiva de conjunto dos números naturais. "Caracterizar completamente" significa que um conjunto obedecendo tais axiomas é uma "cópia" daquilo que já conhecemos intuitivamente como conjunto dos números naturais. Mais adiante expressaremos essa semelhança de uma maneira mais precisa.

Essa axiomatização do conjunto dos números naturais é uma adaptação para a

simbologia matemática atual daquela que foi apresentada pelo matemático italiano Giuseppe Peano, no final do século XIX.

2.1 Axiomática de Peano e conjuntos infinitos

Entre as várias ideias que nos vêm à mente ao pensarmos no conjunto dos números naturais, temos: "esse conjunto começa no zero e prossegue de um em um". Uma outra ideia, menos imediata, da qual já ouvimos falar durante a nossa formação matemática é a do *Princípio da Indução Finita.* Imagine que um subconjunto A dos números naturais contém o número 5. Suponha que este subconjunto possui também a seguinte propriedade: ele contém o sucessor natural de qualquer elemento seu, isto é, se $x \in A$, então $x+1 \in A$. Logo, A conterá o 6, pois, pela hipótese inicial, contém o 5. Mas então conterá o 7, pois contém o 6. Portanto, por conter o 7, conterá o 8 e assim por diante. Concluímos que A contém o conjunto $\{5,6,7,8,\ldots\}$. Note, no entanto, que não sabemos se A contém o 4, o 3 etc. Se a nossa hipótese inicial, $5 \in A$, fosse substituída por $0 \in A$, então poderíamos garantir que A seria igual ao conjunto dos números naturais (pois A já fora inicialmente tomado como subconjunto dos naturais).

Os axiomas de Peano são uma apresentação matematicamente rigorosa dessas ideias intuitivas, e se apoiam em conceitos matemáticos que já conhecemos ou admitimos conhecidos, no caso, o de conjunto e de função. Vamos então a esta apresentação:

Existe um conjunto $\mathbb{N}$ e uma função $s : \mathbb{N} \rightarrow \mathbb{N}$ verificando:

A_1) s é injetora;

A_2) Existe um elemento em $\mathbb{N}$, que denotaremos por 0, e chamaremos de zero, que não está na imagem de s, isto é, $0 \notin Im(s)$.

Antes de enunciarmos o 3º e último axioma de Peano, vamos tentar perceber que tipo de ideia está por trás da função s. Este "s" vem da palavra sucessor, de modo que se $x \in \mathbb{N}$, $s(x)$ será chamado de *sucessor de x*. Assim, o primeiro axioma nos diz que elementos diferentes de $\mathbb{N}$ possuem sucessores diferentes, enquanto o segundo axioma expressa o fato de que 0 não é sucessor de nenhum elemento de $\mathbb{N}$.

Veremos adiante que $s(x)$ é o sucessor natural de x que conhecemos intuitivamente, isto é, $x+1$. Mas cuidado! Em nosso contexto axiomático ainda não definimos adição, e nem sabemos o que significa o símbolo "1". Por isso confirmaremos essa afirmação posteriormente, na Proposição 2.2.1. Vamos agora ao último axioma de Peano.

A_3) Se um subconjunto X de $\mathbb{N}$ satisfizer (i) e (ii) abaixo, então $X = \mathbb{N}$:

i) $0 \in X$;

ii) Se $k \in X$, então $s(k) \in X$.

$\mathbb{N}$ se chama *Conjunto dos Números Naturais*. O axioma A_2 garante que $\mathbb{N} \neq \emptyset$, pois $0 \in \mathbb{N}$. Além disso, como $s(0) \neq 0$ (pois $0 \notin$ Im(s) e $s(0) \in$ Im(s)), então $\mathbb{N}$ contém pelo menos dois elementos: 0 e $s(0)$.

Ainda estamos um pouco longe do nosso conjunto intuitivo dos números naturais, com seus "infinitos" elementos. Entretanto, observe que $s(s(0))$ é diferente de

0 (porque $0 \notin \text{Im}(s)$) e de $s(0)$ (pois s é injetora ($0 \neq s(0) \Rightarrow s(0) \neq s(s(0))$)). Isso acrescenta mais um elemento em $\mathbb{N}$, a saber, $s(s(0))$.

De maneira análoga, a imagem de $s(s(0))$ por s também está em $\mathbb{N}$ e é diferente dos elementos $0, s(0), s(s(0))$, já mencionados. (Verifique!)

Tomando então sucessores de forma iterada, parece que cada elemento novo é diferente de todos aqueles anteriormente obtidos. De fato, isso ocorre e será provado rigorosamente na Proposição 2.3.6, quando tivermos à disposição a notação adequada para expressar as estruturas aritmética e de ordem de $\mathbb{N}$. Devido a esse fato é que consideramos $\mathbb{N}$ infinito e, de modo geral, definimos conjunto infinito como segue:

Definição 2.1.1. Um conjunto X diz-se *infinito* quando existe uma função injetora $f : \mathbb{N} \to X$. Um conjunto é dito *finito* quando não for infinito. Ou seja, um conjunto é infinito quando contiver um subconjunto Y em bijeção com $\mathbb{N}$, o que também se expressa dizendo que Y é *equipotente* a $\mathbb{N}$.

Assim, se considerarmos por um momento a noção intuitiva dos conjuntos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$, é imediato que todos eles são infinitos, conforme comprovaremos rigorosamente nos capítulos seguintes.

Há outras definições de conjuntos infinitos (portanto, de conjuntos finitos) obviamente equivalentes à que demos acima. Vale a pena comentar uma delas, que é devida a Cantor, porque ela rompeu com o paradigma milenar grego de que "o todo é sempre maior do que qualquer uma de suas partes próprias": Um conjunto diz-se infinito quando existir uma bijeção entre ele e um subconjunto próprio dele.

Assim, o Teorema 2.1.1 adiante nos garantirá, novamente, que $\mathbb{N}$ é infinito, pois provaremos que a função $s : \mathbb{N} \to \mathbb{N}^*$ é uma bijeção.

Admitindo-se a notação usual para os números naturais (veja seção 2.2.1), pode-se provar ainda que um conjunto X é finito se, e somente se, ele for vazio ou estiver em bijeção com um conjunto do tipo $I_n = \{1,2,3,...,n\}$, para algum $n \in \mathbb{N}^*$. Um tal n, quando existe, é único e chama-se *número de elementos de* X. Além disso, todo subconjunto de um conjunto finito é finito, em plena concordância com o nosso conceito intuitivo de finitude.

Para a demonstração rigorosa dessas afirmações, bem como para mais detalhes sobre as propriedades de conjuntos finitos e infinitos, veja, por exemplo, os itens [22] e [30] da bibliografia.

O axioma A_3 acima é conhecido na literatura como o Princípio da Indução Finita, ou Princípio da Indução Matemática, ou Princípio da Indução Completa, ou simplesmente *Princípio da Indução*. Ele é utilizado como método de demonstração de teoremas que dizem respeito a propriedades do conjunto dos números naturais, conforme veremos adiante.

Sabemos, pelo axioma A_2, que $0 \notin \text{Im}(s)$. Mas o que é $\text{Im}(s)$? O item (ii) do teorema abaixo responde a esta questão:

Teorema 2.1.1. *Se $s : \mathbb{N} \to \mathbb{N}$ é a função sucessor, então, tem-se:*

i) $s(n) \neq n$, para todo $n \in \mathbb{N}$ (nenhum número natural é sucessor de si mesmo);

ii) $Im(s) = \mathbb{N} \setminus \{0\}$ (0 é o único número natural que não é sucessor de nenhum número natural).

Demonstração.

i) Seja A o subconjunto de $\mathbb{N}$ constituído dos elementos $n \in \mathbb{N}$ tais que $s(n) \neq n$. Usaremos o Princípio da Indução para mostrarmos que $A = \mathbb{N}$, ou seja, $s(n) \neq n$, $\forall n \in \mathbb{N}$. Temos: $0 \in A$, pois $s(0) \neq 0$ já que $0 \notin \mathrm{Im}(s)$, por A_2. Verifiquemos agora que vale a implicação: $k \in A \Rightarrow s(k) \in A$. De fato:

$$k \in A \Leftrightarrow s(k) \neq k.$$

Aplicando s em ambos os membros de $s(k) \neq k$, obtemos $s(s(k)) \neq s(k)$, pois s é injetora. Logo $s(k) \in A$. Pelo Princípio da Indução, $A = \mathbb{N}$.

ii) Novamente, usaremos o Princípio da Indução no conjunto

$A = \{0\} \cup \mathrm{Im}(s)$ $(\subset \mathbb{N})$:

$0 \in A$ e $(k \in A \Rightarrow s(k) \in \mathrm{Im}(s) \subset A)$.

Logo $A = \mathbb{N}$ e como $0 \notin \mathrm{Im}(s)$, então $\mathrm{Im}(s) = \mathbb{N} \setminus \{0\}$. □

Denotaremos $\mathbb{N} \setminus \{0\}$ por $\mathbb{N}^*$, conforme notação introduzida no início da seção 1.2. Todo elemento de $\mathbb{N}^*$ é sucessor de um único número natural, que se chama seu *antecessor*.

2.2 Operações com números naturais

Nesta seção, definiremos duas operações sobre o conjunto dos números naturais, que chamaremos de adição (+) e de multiplicação (·). Trata-se de uma primeira formalização das operações de mesmo nome que já conhecemos da matemática elementar.

2.2.1 Adição de números naturais

Definição 2.2.1. A *adição* de dois números naturais, m e n, é designada por $m+n$ e definida *recursivamente* do seguinte modo:

$$\begin{cases} m+0 &= m; \\ m+s(n) &= s(m+n). \end{cases}$$

A definição acima nos fornece, então, a soma de um número arbitrário m com 0: $m+0=m$.

Ela nos dá também a soma de m com $s(0)$:

$$m+s(0)=s(m+0)=s(m).$$

Temos ainda: $m+s(s(0))=s(m+s(0))=s(s(m))$ e assim por diante.

A formalização desse processo se dá através do Princípio da Indução e nos mostra que a soma $m+n$ está definida para todo par m,n de naturais. De fato, para cada m natural fixado arbitrariamente, definimos o conjunto $S_m = \{n \in \mathbb{N} \mid m+n \text{ está definida}\}$. Temos que $0 \in S_m$ e se $k \in S_m$, então $s(k) \in S_m$, pois $m+s(k)=s(m+k)$. Logo, por A_3, $S_m=\mathbb{N}$. Como m é arbitrário, $S_m=\mathbb{N}$, para todo $m \in \mathbb{N}$, ou seja, $m+n$ está definida para todo par (m,n) de naturais, o que nos diz que a adição acima definida é de fato uma operação em $\mathbb{N}$.

Um comentário acerca da definição de adição acima (que se aplica também a outras definições apresentadas de forma recursiva, como a multiplicação de naturais, de potências com expoente natural, de composição interada de funções etc): é possível mostrar que existe uma única operação em $\mathbb{N}$, ou seja, uma função $*: \mathbb{N}\times\mathbb{N} \longrightarrow \mathbb{N}$, que possui as propriedades que utilizamos para definir adição, isto é, $m*0=m$ e $m*s(n)=s(m*n)$. Esse resultado, bem como resultados similares

relativos às outras situações acima mencionadas, são casos particulares de um teorema sobre *funções recursivas* que optamos por não abordar em detalhes neste livro, mas que pode ser apreciado em textos de lógica matemática e de fundamentos da matemática como, por exemplo, nos itens bibliográficos [4], [7], [20] e [26] .

Introduzimos agora a familiar notação para os números naturais, que conhecemos desde nossa infância.

Definição 2.2.2. Indicaremos por 1 (lê-se "um") o número natural que é sucessor de 0, ou seja, $1 = s(0)$.

Confirmando o que dissemos antes de enunciar o Axioma A_3, temos:

Proposição 2.2.1. *Para todo natural m, tem-se* $s(m) = m+1$ *e* $s(m) = 1+m$*. Portanto,* $m+1 = 1+m$*.*

Demonstração. Para a primeira igualdade, temos: $m+1 = m+s(0) = s(m+0) = s(m)$.

Para a segunda igualdade, consideremos o conjunto $A = \{m \in \mathbb{N} \,|\, s(m) = 1+m\}$. Claramente, $0 \in A$, pois $s(0) = 1 = 1+0$. Seja $m \in A$. Vamos mostrar que $s(m) \in A$. De fato, como $s(m) = 1+m$, temos que

$$s(s(m)) = s(1+m) = 1+s(m),$$

isto é, $s(m) \in A$. Assim, pelo Axioma A_3, temos $A = \mathbb{N}$. □

Como era de se esperar, passaremos a adotar a notação indo-arábica (de base dez) para os elementos de $\mathbb{N}$ (Maiores detalhes sobre sistemas de numeração serão considerados na seção 5.3.).

Já temos os símbolos 0 e $1 = s(0)$. Definimos:

$$s(1) = 2 \quad \text{(lê-se dois);}$$

$$s(2) = 3 \quad \text{(lê-se três);}$$

$$s(3) = 4 \quad \text{(lê-se quatro);}$$

$$s(4) = 5 \quad \text{(lê-se cinco);}$$

e assim por diante. Então, vemos que $\mathbb{N}$ contém o conjunto

$$\{0, s(0), s(s(0)), s(s(s(0))), \ldots\} = \{0, 1, 2, 3, \ldots\}.$$

A questão que se coloca agora é: $\mathbb{N}$ contém outros elementos além desses? Se a resposta for negativa, teremos concluído que os axiomas de Peano realmente formalizam a nossa ideia intuitiva de conjunto dos números naturais.

Teorema 2.2.2. $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$.

Demonstração. Seja S o conjunto $\{0, 1, 2, 3, \ldots\}$. Na verdade, S foi construído como um subconjunto de $\mathbb{N}$ que contém o 0 e também o sucessor de qualquer elemento nele contido. Pelo Princípio da Indução, $S = \mathbb{N}$. □

Note que $0 \neq 1$, mas não sabemos ainda comparar 0 com 1, isto é, não formalizamos ainda a ideia intuitiva de que 1 é maior do que 0. Isso decorrerá a partir da definição de uma *relação de ordem* em $\mathbb{N}$, que estabeleceremos posteriormente.

Ilustraremos agora algumas adições em $\mathbb{N}$, utilizando a notação anterior:

1) $1 + 1 = s(1) = 2$.

2) $2 + 1 = s(2) = 3$.

3) $2 + 2 = 2 + s(1) = s(2 + 1) = s(2 + s(0)) = s(s(2 + 0)) = s(s(2)) = s(3) = 4$.

4) $0+2=0+s(1)=s(0+1)=s(1+0)=s(1)=2.$

(Na terceira igualdade de (4), usamos a Proposição 2.2.1.)

Antes de estudar mais exemplos, vamos lembrar a notação usual de composição iterada de funções através da definição seguinte, onde f é uma função de um conjunto X nele próprio e Id_X é a função identidade no conjunto X:

$$f^0 = Id_X \text{ e, para } n \geq 1,\ f^n = f \circ (f^{n-1}).$$

Assim, temos: $f^1 = f$, $f^2 = f \circ f$, $f^3 = f \circ (f \circ f)$ etc. A função f^n se diz a *n-ésima iterada de* f, em cujo caso também se diz que f *foi iterada* n *vezes.*

Exercício 16. Mostre por indução que, para m e n naturais, vale a igualdade $m+n = s^n(m)$, isto é, somar n a m é somar 1 a m iteradamente n vezes.

Exercício 17. Assumindo conhecido o sistema de numeração decimal indo-arábico (conforme seção 5.3), efetue:

1) $3+4$

2) $27+12$

Algumas das propriedades da adição, que admitíamos como intuitivamente óbvias, são demonstradas no teorema seguinte com base nos axiomas de Peano e nas definições precedentes.

Observe a importância do Princípio da Indução em todas as demonstrações que se seguem.

Teorema 2.2.3. *Sejam m, n e p números naturais arbitrários. São verdadeiras as afirmações:*

i) Propriedade associativa da adição: $m+(n+p)=(m+n)+p$.

ii) Propriedade comutativa da adição: $n+m=m+n$.

iii) Lei do cancelamento da adição: $m+p=n+p \Rightarrow m=n$.

Demonstração. Mostraremos (i) e indicaremos um roteiro para a demonstração de (ii) e (iii) nos exercícios a seguir.

Fixemos os naturais m e n e apliquemos indução sobre p.

Seja $A_{(m,n)}=\{p\in\mathbb{N}\,|\,m+(n+p)=(m+n)+p\}$.

Temos, $0\in A_{(m,n)}$, pois $m+(n+0)=(m+n)+0$, pela definição de adição. Mostremos agora que o fato de k pertencer a $A_{(m,n)}$ acarreta que $s(k)$ pertence a $A_{(m,n)}$:

$m+(n+s(k))=m+s(n+k)=s(m+(n+k))=s((m+n)+k)=(m+n)+s(k)$.

Portanto, $A_{(m,n)}=\mathbb{N}$. Como m e n são arbitrários, obtemos (i). □

A propriedade associativa da adição permite-nos interpretar uma *adição de três parcelas* $a+b+c$ como sendo a adição $(a+b)+c$ ou a adição $a+(b+c)$. Na verdade, um cuidadoso argumento usando indução permite provar a *lei associativa generalizada da adição*, segundo a qual, para $m_1,m_2,...,m_k$ naturais, a expressão $m_1+m_2+...+m_k$ pode ser interpretada como sucessivas adições com os parênteses em qualquer posição, pois seu valor é independente dessas posições. Assim, por exemplo, a adição de naturais $a+b+c+d$ pode ser interpretada como $((a+b)+c)+d$ ou $a+((b+c)+d)$ etc. (Consulte [9] para uma demonstração

desse fato no contexto mais geral de Teoria dos Grupos. Esse teorema permite aplicar a observação acima a todas as situações neste livro em que ocorrer uma operação associativa, ou seja, nelas valerá também a correspondente *lei associativa generalizada.*)

Exercício 18. Mostre que $m+0=0+m$, para todo $m \in \mathbb{N}$, isto é, 0 é um *elemento neutro* para a operação de adição em $\mathbb{N}$.

Exercício 19. Para provar a propriedade comutativa da adição, fixe arbitrariamente $m \in \mathbb{N}$ e considere o conjunto $C_m = \{n \in \mathbb{N} \mid n+m = m+n\}$. Mostre por indução que $C_m = \mathbb{N}$.

(Sugestão: Use o Exercício 18, a propriedade associativa da adição e a Proposição 2.2.1.)

Exercício 20. Prove a lei do cancelamento da adição.

Proposição 2.2.4. *Suponha que exista $u \in \mathbb{N}$ tal que $m+u=m$ (ou que $u+m=m$), para todo $m \in \mathbb{N}$. Então $u=0$. Assim, 0 é o **único** elemento neutro para a operação de adição (veja o Exercício 18).*

Demonstração. Para um tal u, temos: $0 = 0+u = u$. □

A proposição acima permite uma generalização conforme o Exercício 38 no capítulo 3.

2.2.2 Multiplicação de números naturais

Definição 2.2.3. A *multiplicação* de dois números naturais, m e n, é designada por $m \cdot n$ e definida *recursivamente* do seguinte modo:

$$\begin{cases} m \cdot 0 &= 0; \\ m \cdot (n+1) &= m \cdot n + m \end{cases}$$

Como de costume, adotaremos a notação de justaposição para a multiplicação:

$$m \cdot n = mn.$$

Observe que na própria definição de multiplicação estão os cernes da propriedade distributiva da multiplicação em relação à adição e da propriedade do elemento neutro multiplicativo, conforme os itens (iii) e (ii) do teorema abaixo.

Esta definição nos fornece a multiplicação de um número natural arbitrário m por 0. Note no entanto que não é tão óbvio que $0 \cdot m = 0$. Este fato será considerado no Exercício 24.

As propriedades da multiplicação são enunciadas no teorema a seguir.

Teorema 2.2.5. *Para m, n e p naturais arbitrários, valem as proposições abaixo:*

i) $mn \in \mathbb{N}$, *isto é, a multiplicação de fato é uma operação em* $\mathbb{N}$;

ii) *existência do elemento neutro multiplicativo:* $1 \cdot n = n \cdot 1 = n$;

iii) *distributividade:* $m(n+p) = mn + mp$ *e* $(m+n)p = mp + np$;

iv) *associatividade:* $m(np) = (mn)p$;

v) $mn = 0 \Rightarrow m = 0$ *ou* $n = 0$*;*

vi) comutatividade: $nm = mn$.

Demonstração. Novamente, usa-se o Princípio da Indução para demonstrar todos os seis itens. Demonstraremos os itens (ii) e (iii) e deixaremos os demais para os exercícios seguintes.

ii) Mostremos inicialmente que $n \cdot 1 = n$:

$$n \cdot 1 = n(0+1) = n \cdot 0 + n = 0 + n = n$$

(Usamos a definição de multiplicação na segunda e terceira igualdades acima).

Mostremos agora, por indução em n, que $1 \cdot n = n$. Temos: $1 \cdot 0 = 0$, por definição e, sob a hipótese de que $1 \cdot n = n$, obtemos: $1 \cdot (n+1) = 1 \cdot n + 1 = n + 1$.

iii) Sejam m e n naturais fixados arbitrariamente e usemos indução sobre p. Seja $P_{m,n}(p)$ a afirmação $m(n+p) = mn + mp$. Mostraremos que o conjunto $A_{m,n} = \{p \in \mathbb{N} \mid P_{m,n}(p) \text{ é verdadeira}\}$ é $\mathbb{N}$. Temos:

1) $P_{m,n}(0)$ é verdadeira:

$$m(n+0) = mn \qquad \text{e} \qquad mn + m \cdot 0 = mn + 0 = mn.$$

Logo, $m(n+0) = mn + m \cdot 0$, isto é, $P_{m,n}(0)$ é verdadeira.

2) Mostremos que $P_{m,n}(k+1)$ pode se obter de $P_{m,n}(k)$, isto é, que $k \in A_{m,n}$ acarreta $k+1 \in A_{m,n}$. Cada igualdade abaixo se justifica com base em propriedades já estabelecidas (verifique): $m(n+(p+1)) = m((n+p)+1) = m(n+p)+m = (mn+mp)+m = mn+(mp+m) = mn+(m(p+1))$.

De 1) e 2), concluímos, por indução, que $A_{m,n} = \mathbb{N}$. □

Exercício 21. Demonstre o item (iv) do teorema acima. (Sugestão: use indução sobre p.)

Exercício 22. Mostre que o elemento neutro multiplicativo é único, isto é, se $p \in \mathbb{N}$ é tal que $np = n$ (ou $pn = n$), para todo $n \in \mathbb{N}$, então $p = 1$. Compare com a Proposição 2.2.4.

Proposição 2.2.6. *Sejam* m*,* $n \in \mathbb{N}$ *tais que* $m + n = 0$*. Então* $m = n = 0$*.*

Demonstração. Suponhamos $n \neq 0$. Então $n = s(n') = n' + 1$, para algum $n' \in \mathbb{N}$. Temos:

$$0 = m + n = m + (n' + 1) = (m + n') + 1 = s(m + n'),$$

o que é absurdo, pois zero não é sucessor de nenhum número. Logo, $n = 0$ e obtemos $m = m + 0 = m + n = 0$, como queríamos. □

Exercício 23. Com o auxílio da proposição acima e da propriedade (iii) do Teorema 2.2.5, prove a propriedade (v).

(Sugestão: suponha $n \neq 0$, isto é, $n = n' + 1$, para certo $n' \in \mathbb{N}$. Conclua que m deve ser 0.)

Exercício 24. Mostre que $0 \cdot m = 0$, para todo $m \in \mathbb{N}$.

Exercício 25. Demonstre a comutatividade da multiplicação, isto é, $mn = nm$, para todo par n, m de números naturais.

(Sugestão: fixe m arbitrariamente e use indução sobre n.)

2.3 Relação de ordem em $\mathbb{N}$

A relação de ordem em $\mathbb{N}$ nos permitirá comparar os números naturais, formalizando a ideia intuitiva de que 0 é menor do que 1, que é menor do que 2, e assim por diante.

Definição 2.3.1. Uma relação binária R em um conjunto não vazio A diz-se uma *relação de ordem em* A quando satisfizer as condições seguintes, para quaisquer $x, y, z \in A$:

i) *reflexividade*: xRx.

ii) *antissimetria*: se xRy e yRx, então $x = y$.

iii) *transitividade*: se xRy e yRz, então xRz.

Um conjunto não vazio A, munido de uma relação de ordem, diz-se um *conjunto ordenado*.

Definiremos agora uma relação de ordem em $\mathbb{N}$ através da operação da adição, tornando-o, portanto, um conjunto ordenado.

Definição 2.3.2. Dados $m, n \in \mathbb{N}$, dizemos que mRn se existir $p \in \mathbb{N}$ tal que $n = m + p$.

Exemplo 2.3.1. $1R3$, pois $3 = 1 + 2$; $2R2$, pois $2 = 2 + 0$.

Exercício 26. Mostre que R é uma relação de ordem em $\mathbb{N}$.

Definição 2.3.3. Para $m, n \in \mathbb{N}$, se mRn, onde R é a relação da definição anterior, dizemos que *m é menor do que ou igual a n* e passaremos a escrever o símbolo $\leq$ no lugar de R: assim, $m \leq n$ significará mRn.

(A expressão "*m é menor ou igual a n*", embora gramaticalmente incorreta, é de uso corrente desde o Ensino Fundamental.)

Notação:

1. Se $m \leq n$, mas $m \neq n$, escrevemos $m < n$ e dizemos que *m é menor do que n.*

2. Escrevemos $n \geq m$ como alternativa a $m \leq n$. Leremos *n é maior do que ou igual a m.*

3. Escrevemos $n > m$ como alternativa a $m < n$. Leremos *n é maior do que m.*

Exercício 27. Mostre que, para todo $n \in \mathbb{N}^*$, $n > 0$. Em particular, $1 > 0$.

Exercício 28. Mostre que $s(n) > n$, para todo $n \in \mathbb{N}$.

Proposição 2.3.1. *(Lei da Tricotomia) Para quaisquer $m, n \in \mathbb{N}$, temos que uma, e apenas uma, das relações seguintes ocorre:*

i) $m < n$;

ii) $m = n$;

iii) $m > n$.

Demonstração. Mostremos inicialmente que duas dessas relações não podem ocorrer simultaneamente. Depois, mostraremos que uma delas necessariamente ocorre. É claro que (i) e (ii), bem como (ii) e (iii), são incompatíveis, por definição. Quanto a (i) e (iii) ocorrendo simultaneamente, teríamos: $n = m + p$ e $m = n + p'$, com $p, p' \neq 0$, de onde obtemos:

$$n + 0 = n = (n + p') + p = n + (p' + p).$$

Cancelando n, obtemos $p + p' = 0$. Pela Proposição 2.2.6, segue que $p = p' = 0$, uma contradição.

Mostremos agora que uma das três relações acontece. Seja m um natural arbitrário e consideremos o conjunto $M = \{x \in \mathbb{N} \mid x = m \text{ ou } x > m \text{ ou } x < m\}$. Vamos provar, por indução sobre x, que $M = \mathbb{N}$.

Temos que $0 \in M$, pois $0 = m$ ou $0 \neq m$. No último caso, pelo Exercício 27, $m > 0$.

Mostremos agora que a hipótese $k \in M$ acarreta $k+1 \in M$. Devemos considerar três situações:

1ª) $k = m$. Neste caso, $k+1 = m+1$, de onde $k+1 > m$ e, portanto, $k+1 \in M$.

2ª) $k > m$. Neste caso, existe $p \in \mathbb{N}^*$ tal que $k = m+p$. Então $k+1 = (m+p)+1 = m+(p+1)$, de onde $k+1 > m$ e, daí, $k+1 \in M$.

3ª) $k < m$. Neste caso, existe $p \in \mathbb{N}^*$ tal que $m = k+p$. Como $p \neq 0$, então $p = p'+1$, $p' \in \mathbb{N}$. Logo

$$m = k+(p'+1) = k+(1+p') = (k+1)+p'.$$

Se $p' = 0$, então $m = k+1$ e $k+1 \in M$. Se $p' \neq 0$, então $m > k+1$ e $k+1 \in M$.

Assim, pelo Princípio da Indução, $M = \mathbb{N}$. □

A lei da tricotomia equivale a dizer que, dados $m, n \in \mathbb{N}$, tem-se, necessariamente $m \leq n$ ou $n \leq m$, isto é, dois naturais quaisquer são sempre comparáveis pela relação de ordem acima definida. Por isso, uma relação de ordem que satisfaz à lei da tricotomia é chamada de *relação de ordem total*. No exercício seguinte, você é convidado a estudar uma relação de ordem em um certo conjunto, que não é total. Nesses casos, a relação de ordem diz-se *parcial*.

Exercício 29. Seja X um conjunto e considere a relação de inclusão entre os subconjuntos de $\mathcal{P}(X)$. Mostre que essa relação é de ordem em $\mathcal{P}(X)$ e que só é de

ordem total nos casos em que X for vazio ou unitário.

Exercício 30. Mostre que a relação de desigualdade estrita em $\mathbb{N}$, isto é, $<$ (ou $>$), é transitiva, mas não é reflexiva nem antissimétrica.

Teorema 2.3.2. *(Compatibilidade da relação de ordem com as operações em* $\mathbb{N}$*) Sejam* a, b *e* c *naturais quaisquer. São válidas as seguintes implicações:*

i) $a \leq b \Rightarrow a + c \leq b + c$*;*

ii) $a \leq b \Rightarrow ac \leq bc$*.*

Demonstração. (i) $a \leq b \Leftrightarrow$ existe $p \in \mathbb{N}$ tal que $b = a + p$. Segue daí que:

$$b + c = (a + p) + c = a + (p + c) = a + (c + p) = (a + c) + p$$

de onde obtemos $b + c \geq a + c$. □

Exercício 31. Demonstre (ii) do teorema anterior.

Exercício 32. Mostre que vale a recíproca do teorema anterior.

Exercício 33.

1) Mostre que o teorema anterior vale com $<$ no lugar de $\leq$ (e $c \neq 0$ no caso (ii)).

2) Conclua que o teorema anterior e o item (1) acima são válidos, respectivamente, com $\geq$ e $>$ no lugar de $\leq$ e $<$.

Teorema 2.3.3. *(Lei do cancelamento da multiplicação) Sejam* $a, b, c \in \mathbb{N}$*, com* $c \neq 0$*, tais que* $ac = bc$*. Então* $a = b$*.*

Demonstração. Se $a > b$, teríamos $ac > bc$ pelo exercício anterior, o que contraria a suposição de que $ac = bc$.

O caso $a < b$ é análogo. Logo, pela lei da tricotomia, $a = b$. □

Teorema 2.3.4. *Sejam* $a, b \in \mathbb{N}$. *Então* $a < b$ *se, e somente se,* $a + 1 \leq b$.

Demonstração. $a < b \Rightarrow b = a + p$, para algum $p \in \mathbb{N}$, $p \neq 0$.

Temos: $p = s(q) = q + 1$, para um certo $q \in \mathbb{N}$. Então

$$b = a + p = a + (q + 1) = a + (1 + q) = (a + 1) + q \Rightarrow b \geq a + 1.$$

A recíproca é imediata. □

Sabemos que $\mathbb{N} = \{0, s(0), s(s(0)), ...\} = \{0, 1, 2, ...\}$, isto é, $\mathbb{N}$ é formado por 0 e pelos seus sucessivos sucessores.

Da relação de ordem em $\mathbb{N}$ e suas propriedades, decorre que $0 < 1 < 2 < 3 < ...$, ou seja, se $a \in \mathbb{N}$, então $a < s(a)$, pois $s(a) = a + 1$.

Além disso, não há naturais compreendidos entre a e $s(a)$, qualquer que seja $a \in \mathbb{N}$, pois $a < r < a + 1$, acarretaria, pelo teorema anterior, $a + 1 \leq r < a + 1$, de onde obtemos (verifique!) $a + 1 < a + 1$, uma contradição.

Assim, vemos que os axiomas de Peano e suas consequências realmente cumprem o objetivo de tornar rigoroso o conceito de número natural, reforçando a observação feita antes do Teorema 2.2.2.

O teorema seguinte também reflete um fato intuitivamente claro desde o Ensino Fundamental: o de que todo subconjunto não vazio de números naturais possui um menor elemento.

Observe que tal propriedade não é verificada no conjunto dos números racionais. Por exemplo, se considerarmos o subconjunto dos números racionais positivos, ele

não possui um menor elemento (Por quê?). Já no conjunto dos números inteiros, só possuem elemento mínimo os subconjuntos que são *limitados inferiormente*, conforme veremos no capítulo seguinte (Teorema 3.3.3).

Formalmente, dizemos que um elemento a de um conjunto ordenado A é um *menor elemento* de A, se $a \leq x$, para todo $x \in A$. Quando um conjunto ordenado A admite um menor elemento, este elemento é único (verifique isso!) e é também chamado de *elemento mínimo* de A. Ele se denota por $\min A$. De modo similar, define-se *maior elemento* ou *elemento máximo* de um conjunto ordenado A, denotado por $\max A$.

Teorema 2.3.5. *(Princípio da Boa Ordem): Todo subconjunto não vazio de números naturais possui um menor elemento.*

Demonstração. Seja S um tal subconjunto de $\mathbb{N}$ e consideremos o conjunto $M = \{n \in \mathbb{N} \mid n \leq x, \forall x \in S\}$. Claro que $0 \in M$. Como $S \neq \varnothing$, tome $s \in S$. Então $s+1 \notin M$, pois $s+1$ não é menor ou igual a s. Assim, $M \neq \mathbb{N}$. Como $0 \in M$ e $M \neq \mathbb{N}$, deve existir $m \in M$ tal que $m+1 \notin M$, caso contrário, pelo Princípio de Indução, M deveria ser $\mathbb{N}$.

Afirmamos que um tal m é o menor elemento de S, isto é , $m = \min S$.

Como $m \in M$, então $m \leq x$, $\forall x \in S$. Só falta verificar que $m \in S$. Vamos supor o contrário, que $m \notin S$. Então $m < x$, $\forall x \in S$.

Pelo teorema anterior, teríamos $m+1 \leq x$, $\forall x \in S$, do que resultaria $m+1 \in M$, em contradição com a escolha de m.

Logo $m \in S$, conforme queríamos. □

O nome "Princípio da Boa Ordem" para o teorema anterior deve-se à íntima

relação desse teorema com o fato de que dado um número natural arbitrário n, o próximo natural maior do que n está determinado e é $n+1$, como demonstrado no Teorema 2.3.4, que foi utilizado no último argumento da demonstração acima. Observe que o Teorema 2.3.4 não se aplica, por exemplo, ao conjunto dos números racionais: é possível determinar um número racional imediatamente maior do que 1?

Um outro fato que foi utilizado para demonstrar o Princípio da Boa Ordem foi o Princípio da Indução, ou seja, o Princípio da Indução implica no da Boa Ordem. Na verdade, o Princípio da Indução e o da Boa Ordem são proposições matemáticas equivalentes. Isso significa o seguinte: provamos o Princípio da Boa Ordem a partir do Princípio da Indução (e dos demais axiomas de Peano). Se tivéssemos admitido como axioma o Princípio da Boa Ordem no lugar do Princípio da Indução, o último poderia ter sido demonstrado como teorema (veja [22]). Além disso, obteríamos os mesmos resultados que obtivemos, isto é, o mesmo conjunto de números naturais com as mesmas propriedades.

Exercício 34. Sejam x e y números naturais. Mostre que:

1. $x+y=1 \Rightarrow x=1$ ou $y=1$.

2. Se $x \neq 0$, $y \neq 0$ e $x+y=2$, então $x=y=1$.

3. $xy \neq 0 \Rightarrow x \leq xy$.

Exercício 35. Para $x,y,z \in \mathbb{N}$, mostre que se $x+z < y+z$ então $x < y$.

Exercício 36. Para $x,y \in \mathbb{N}$ e $z \in \mathbb{N}^*$, mostre que se $xz \leq yz$ então $x \leq y$.

Vamos demonstrar na próxima proposição que o processo de tomar sucessores de forma iterada produz elementos distintos dos anteriormente produzidos. Usaremos aqui a notação de composição iterada de funções introduzida na seção 2.2.1.

Exercício 37. Seja X um subconjunto de $\mathbb{N}$ satisfazendo (i) e (ii) abaixo. Mostre que $\{a, a+1, a+2, \ldots\} \subset X$:
(i) $a \in X$ (ii) $n \in X \Rightarrow n+1 \in X$
(Sugestão: aplique o Princípio da Indução ao conjunto $Y = \{m \in \mathbb{N} \mid a+m \in X\}$.)

Proposição 2.3.6. *Seja* $s : \mathbb{N} \to \mathbb{N}$ *a função sucessor. Para cada* $n \geq 1$*, tem-se* $s^n(0) \neq s^k(0)$*, para todo* $k < n$*.*

Demonstração. Seja $X = \{n \in \mathbb{N}^* \mid s^n(0) \neq s^k(0), \forall k < n\}$. Mostremos, usando o Exercício 37, que $X = \mathbb{N}^*$. Temos:
(i) $1 \in X$, pois $s^1(0) = s(0) = 1 \neq 0 = s^0(0)$;
(ii) Seja $n \in X$, isto é, $s^n(0) \neq s^k(0)$, para todo $k < n$.

Mostremos que $n+1 \in X$, de onde decorrerá, pelo Exercício 37, que $X = \mathbb{N}^*$.

Aplicando s (injetora) a ambos os membros da desigualdade acima, obtemos: $s^{n+1}(0) \neq s^{k+1}(0)$, para todo $k < n$, o que é o mesmo que $s^{n+1}(0) \neq s^l(0)$, para todo l de 1 até n. Como também $s^{n+1}(0) \neq 0 = s^0(0)$, concluímos que $s^{n+1}(0) \neq s^l(0)$, para todo $l < n+1$, o que diz que $n+1 \in X$, como queríamos. □

3

Números inteiros

Em $\mathbb{N}$ estão definidas duas operações que denominamos de adição e multiplicação. No Ensino Fundamental, os números inteiros negativos e suas propriedades são introduzidos para dar significado a certas subtrações, do tipo: $3-5$, $8-13$ etc.

Uma vez introduzidos tais números, são "definidas" as demais operações com eles, como: $3-(-5)$, $(-8)\cdot(-3)$, $8\div(-4)$, $(-2)^3$ etc. As aspas devem-se ao fato de que tais "definições" são dadas de modo ingênuo, não rigoroso, numa tentativa de estender as operações aritméticas e suas propriedades no conjunto $\mathbb{N}$ para o conjunto $\mathbb{Z}$. E é isso mesmo o que está acessível ao estudante do Ensino Fundamental (embora mais se espere de seu professor de matemática, para quem este livro foi escrito).

Foi também dessa forma empírica que os números inteiros negativos foram descobertos e aplicados na expressão matemática de certas situações e na resolução de problemas.

Do ponto de vista do rigor matemático, apenas admitir a existência de números inteiros negativos e incorporá-los ao conjunto $\mathbb{N}$ não é adequado. Além disso, temos em $\mathbb{N}$ as operações de adição e multiplicação. A subtração, como a entendemos da

matemática elementar, não é, a rigor, uma operação em $\mathbb{N}$, conforme o Exercício 6. Por essas razões, não seguiremos a linha adotada no Ensino Fundamental. O que faremos é *construir* esses números negativos a partir da estrutura aritmética que temos em $\mathbb{N}$, através das noções básicas de Teoria dos Conjuntos e de relações de equivalência.

3.1 Construção do conjunto dos números inteiros

Começaremos definindo uma relação de equivalência no conjunto $\mathbb{N} \times \mathbb{N}$. Um número inteiro será então definido como uma classe de equivalência dada por essa relação. O conjunto $\mathbb{Z}$ dos números inteiros será portanto o conjunto dessas classes de equivalência. Definiremos duas operações aritméticas em $\mathbb{Z}$ e mostraremos que $\mathbb{Z}$ contém uma *cópia algébrica* de $\mathbb{N}$, num sentido que precisaremos oportunamente. Por fim, definiremos a operação de subtração em $\mathbb{Z}$ que, restrita a elementos da cópia de $\mathbb{N}$ em $\mathbb{Z}$, trará significado às operações do tipo $3-5$ e às demais operações comentadas acima.

Teorema 3.1.1. *A relação* $\sim$ *em* $\mathbb{N} \times \mathbb{N}$ *definida por* $(a,b) \sim (c,d)$ *quando* $a+d = b+c$ *é de equivalência.*

Um comentário antes da demonstração formal: se admitirmos por um momento a nossa noção intuitiva de números inteiros e de subtração, notamos que $a+d = b+c \Leftrightarrow a-b = c-d$, isto é, dois pares ordenados são equivalentes segundo a definição acima, quando a diferença entre suas coordenadas, na mesma ordem, coincidem.

É esta a forma que os matemáticos do final do século XIX encontraram para iniciar a construção do conjunto $\mathbb{Z}$ sem mencionar subtração, mas trazendo na sua essência o germe dessa operação, tendo como ponto de partida o conjunto $\mathbb{N}$ e suas operações, as noções de produto cartesiano e de relação de equivalência, como mostra a definição dada no Teorema 3.1.1.

Demonstração.

(i) Reflexividade: $(a,b) \sim (a,b)$, pois $a+b=b+a$.

Assim, a reflexividade de $\sim$ é herança da comutatividade da adição em $\mathbb{N}$.

(ii) Simetria: $(a,b) \sim (c,d) \Rightarrow (c,d) \sim (a,b)$.

Basta observar que a implicação acima equivale à implicação $a+d=b+c \Rightarrow c+b=d+a$, que decorre da comutatividade da adição em $\mathbb{N}$.

(iii) Transitividade: $(a,b) \sim (c,d)$ e $(c,d) \sim (e,f) \Rightarrow (a,b) \sim (e,f)$.

A verificação dessa propriedade é um exercício para o leitor. □

Denotaremos por $\overline{(a,b)}$ a *classe de equivalência* do par ordenado (a,b) pela relação $\sim$, isto é,

$$\overline{(a,b)} = \{(x,y) \in \mathbb{N} \times \mathbb{N} \mid (x,y) \sim (a,b)\}.$$

Por exemplo:

i) $\overline{(3,0)} = \{(3,0),(4,1),(5,2),(6,3),\ldots\};$

ii) $\overline{(0,3)} = \{(0,3),(1,4),(2,5),(3,6),\ldots\};$

iii) $\overline{(5,2)} = \{(3,0),(4,1),(5,2),(6,3),\ldots\}.$

Note que $\overline{(5,2)} = \overline{(3,0)}$, o que não é uma surpresa, devido ao Teorema 1.2.2 - (ii).

Definição 3.1.1. O conjunto quociente $\mathbb{N} \times \mathbb{N}/\sim$, constituído pelas classes de equivalência $\overline{(a,b)}$, se denota por $\mathbb{Z}$ e será chamado de *conjunto dos números inteiros.*

Assim,

$$\mathbb{Z} = (\mathbb{N} \times \mathbb{N}/\sim) = \{\overline{(a,b)} \mid (a,b) \in \mathbb{N} \times \mathbb{N}\}.$$

O símbolo $\mathbb{Z}$ tem origem na palavra alemã *"zahl"*, que quer dizer *número.*

3.2 Operações em $\mathbb{Z}$

Definiremos a seguir duas operações em $\mathbb{Z}$, $(+)$ e $(\cdot)$, que denominaremos de *adição* e de *multiplicação*, respectivamente.

3.2.1 Adição de números inteiros

Conforme observamos após o enunciado do Teorema 3.1.1, permitindo-nos usar, por um momento, a noção intuitiva de subtração em $\mathbb{Z}$, temos: $(a,b) \sim (x,y)$ (que equivale a $\overline{(a,b)} = \overline{(x,y)}$), expressa o fato de que $a - b = x - y$. Vamos utilizar esta observação como ponto de partida para buscar uma definição rigorosa de adição de inteiros. Vejamos o que deveria ser $\overline{(a,b)} + \overline{(c,d)}$.

Se $\overline{(a,b)}$ expressa, em essência, a "diferença" $(a-b)$, e $\overline{(c,d)}$ expressa $(c-d)$, a matemática elementar nos dá $(a-b)+(c-d) = (a+c)-(b+d)$. Esta última expressão se traduz, no nosso contexto, como a classe $\overline{(a+c, b+d)}$.

Passando a limpo, obtemos a definição formal de adição de inteiros, sem mencionar subtrações de naturais nem elementos da matemática elementar. Vamos a ela.

Definição 3.2.1. Dados $\overline{(a,b)}$ e $\overline{(c,d)}$ em $\mathbb{Z}$, definimos a *soma* $\overline{(a,b)}+\overline{(c,d)}$ como sendo o inteiro $\overline{(a+c,b+d)}$.

Ao definirmos objetos que envolvem classes de equivalência, é necessário verificarmos que tais definições não dependem de como representamos as classes. Por exemplo, pela definição acima teríamos que $\overline{(3,5)}+\overline{(4,1)}=\overline{(7,6)}$. No entanto, $\overline{(2,4)}=\overline{(3,5)}$ e $\overline{(3,0)}=\overline{(4,1)}$, logo deveríamos ter $\overline{(2,4)}+\overline{(3,0)}$ também igual a $\overline{(7,6)}$. Pela definição dada, $\overline{(2,4)}+\overline{(3,0)}=\overline{(5,4)}$ que, felizmente, é igual a $\overline{(7,6)}$. Mostraremos agora que isso vale em geral, isto é, a definição dada não depende dos representantes das classes de equivalência envolvidas. Diz-se neste caso que a adição está *bem definida*.

Teorema 3.2.1. *Se* $\overline{(a,b)}=\overline{(a',b')}$ *e* $\overline{(c,d)}=\overline{(c',d')}$, *então* $\overline{(a,b)}+\overline{(c,d)}=\overline{(a',b')}+\overline{(c',d')}$, *isto é, a adição de números inteiros está bem definida.*

Demonstração. Sabemos, do Teorema 1.2.2 (ii) que, como $\overline{(a,b)}=\overline{(a',b')}$, então $(a,b)\sim(a',b')$, isto é,

$$a+b'=b+a'. \tag{3.1}$$

Do mesmo modo, como $\overline{(c,d)}=\overline{(c',d')}$, então $(c,d)\sim(c',d')$, isto é,

$$c+d'=d+c'. \tag{3.2}$$

Temos:

$$\overline{(a,b)}+\overline{(c,d)}=\overline{(a+c,b+d)} \text{ e } \overline{(a',b')}+\overline{(c',d')}=\overline{(a'+c',b'+d')}.$$

Mostremos que os dois segundos membros acima coincidem. Isso equivale a mostrar que $(a+c)+(b'+d')=(b+d)+(a'+c')$. Usando (3.1) e (3.2) temos que:

$$(a+c)+(b'+d')=(a+b')+(c+d')=(b+a')+(d+c')=(b+d)+(a'+c'),$$

como queríamos. □

Teorema 3.2.2. *A operação de adição em $\mathbb{Z}$ é associativa, comutativa, tem $\overline{(0,0)}$ como elemento neutro e vale a lei do cancelamento, como em $\mathbb{N}$. Além disso, vale a propriedade do elemento oposto (ou simétrico, ou inverso aditivo): dado $\overline{(a,b)} \in \mathbb{Z}$, existe um único $\overline{(c,d)} \in \mathbb{Z}$ tal que $\overline{(a,b)}+\overline{(c,d)}=\overline{(0,0)}$. Este $\overline{(c,d)}$ é o elemento $\overline{(b,a)}$.*

Demonstração. Veja os exercícios a seguir. □

Exercício 38. Mostre que se um conjunto não vazio A estiver munido de uma operação $*$, que tem *elemento neutro*, então este elemento neutro é único (n é elemento neutro para $*$ quando $n*a=a*n=a$, para todo $a \in A$).

Exercício 39. Nas condições do Exercício 38, dizemos que o elemento a de A é *inversível* para a operação $*$ se existe $b \in A$ tal que $a*b=b*a=n$. Neste caso, b chama-se *inverso* de a (para a operação $*$). Mostre que se a é inversível e $*$ é associativa, então seu inverso é único ($*$ se diz *associativa* se $(a*b)*c=a*(b*c)$, quaisquer que sejam os elementos a,b e c de A. É o que ocorre com as operações definidas nos naturais).

Exercício 40. Nas condições do exercício anterior, tem-se, mais geralmente, o seguinte: se a é inversível e tem b como inverso e se $a * c = n$ (ou $c * a = n$), então $c = b$.

Exercício 41. Demonstre que a adição em $\mathbb{Z}$ é comutativa, associativa e tem $\overline{(0,0)}$ como elemento neutro.

Exercício 42. Demonstre a *lei do cancelamento* para a adição em $\mathbb{Z}$, isto é, se $\alpha, \beta, \gamma \in \mathbb{Z}$ e $\alpha + \beta = \gamma + \beta$, então $\alpha = \gamma$.

Exercício 43. Mostre que $\mathbb{Z}$ possui a propriedade do elemento oposto. Sua unicidade é consequência do Exercício 39.

Definição 3.2.2. Dado $\alpha \in \mathbb{Z}$, o único $\beta \in \mathbb{Z}$ tal que $\alpha + \beta = \overline{(0,0)}$ chama-se *simétrico* de α (ou *oposto* de α, ou *inverso aditivo* de α). Sua unicidade permite que introduzamos um símbolo para ele: $-\alpha$ (lê-se "menos α").

Assim, $\alpha + (-\alpha) = \overline{(0,0)}$. E, como vimos no Teorema 3.2.2, se $\alpha = \overline{(a,b)}$, então $-\alpha = \overline{(b,a)}$.

A existência e unicidade de oposto de um número inteiro permite que definamos uma terceira operação em $\mathbb{Z}$, denominada *subtração*.

Definição 3.2.3. A *subtração* em $\mathbb{Z}$, denotada por $(-)$, é a operação definida da seguinte forma: Se $\alpha, \beta \in \mathbb{Z}$, então:

$$\alpha - \beta = \alpha + (-\beta).$$

Assim, a subtração $\alpha - \beta$ nada mais é do que a soma de α com o simétrico de β.

Proposição 3.2.3. *Para* $\alpha, \beta, \gamma \in \mathbb{Z}$, *vale:*

i) $-(-\alpha) = \alpha$;

ii) $-\alpha + \beta = \beta - \alpha$;

iii) $\alpha - (-\beta) = \alpha + \beta$;

iv) $-\alpha - \beta = -(\alpha + \beta)$;

v) $\alpha - (\beta + \gamma) = \alpha - \beta - \gamma$;

Demonstração. (i) Se $\alpha = \overline{(a,b)}$, então $-(-\alpha) = -\overline{(b,a)} = \overline{(a,b)} = \alpha$.

Outra demonstração deste fato consiste em explorar a propriedade de simétrico: mostrar que $-(-\alpha) = \alpha$ é mostrar que o simétrico de $-\alpha$ é α, o que, por sua vez, significa mostrar que α é o inteiro que somado com $-\alpha$ resulta no neutro $\overline{(0,0)}$, o que decorre imediatamente da propriedade comutativa e da definição de simétrico:

$$-\alpha + \alpha = \alpha + (-\alpha) = \overline{(0,0)}.$$

□

Exercício 44. Demonstre as propriedades de (ii) a (v) do Teorema 3.2.3 acima.

3.2.2 Multiplicação de números inteiros

Com motivações análogas àquelas que consideramos para a definição formal da adição em $\mathbb{Z}$, definimos multiplicação em $\mathbb{Z}$ do seguinte modo:

Definição 3.2.4. Dados $\overline{(a,b)}$ e $\overline{(c,d)}$ em $\mathbb{Z}$, definimos o *produto* $\overline{(a,b)} \cdot \overline{(c,d)}$ como sendo o inteiro $\overline{(ac+bd, ad+bc)}$.

Exercício 45. Faça considerações análogas às que fizemos para a adição para entender a motivação da definição acima.

Exercício 46. Efetue $\overline{(3,5)} \cdot \overline{(10,7)}$.

Como no caso da adição, devemos verificar que a multiplicação está bem definida. Dada a analogia com o caso aditivo, deixaremos como exercício para o leitor a maior parte das demonstrações dos teoremas seguintes.

Teorema 3.2.4. *A multiplicação em $\mathbb{Z}$ está bem definida, isto é, se $\overline{(a,b)} = \overline{(a',b')}$ e $\overline{(c,d)} = \overline{(c',d')}$, então $\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(a',b')} \cdot \overline{(c',d')}$.*

Teorema 3.2.5. *A multiplicação em $\mathbb{Z}$ é comutativa, associativa, tem $\overline{(1,0)}$ como neutro multiplicativo e é distributiva em relação à adição. Além disso, vale a propriedade do cancelamento multiplicativo, isto é, se $\alpha, \beta, \gamma \in \mathbb{Z}$, com $\gamma \neq \overline{(0,0)}$ e $\alpha\gamma = \beta\gamma$, então $\alpha = \beta$.*

Demonstração. (Cancelamento multiplicativo) Sejam $\alpha = \overline{(a,b)}$, $\beta = \overline{(c,d)}$ e $\gamma = \overline{(e,f)} \neq \overline{(0,0)}$ tais que $\alpha\gamma = \beta\gamma$, isto é,

$$\overline{(ae+bf, af+be)} = \overline{(ce+df, cf+de)}$$

que equivale a

$$ae + bf + cf + de = af + be + ce + df.$$

Usando a aritmética dos naturais nessa igualdade, obtemos:

$$e(a+d) + f(b+c) = e(b+c) + f(a+d).$$

Como $\overline{(e,f)} \neq \overline{(0,0)}$, então $e \neq f$. Suponhamos $e > f$, sem perda de generalidade, o que equivale a $e = f + g$, para algum $g \in \mathbb{N}^*$. Substituindo e por $f + g$ na penúltima igualdade, obtemos:

$$f(a+d) + g(a+d) + f(b+c) = f(b+c) + g(b+c) + f(a+d).$$

Usando o cancelamento aditivo em $\mathbb{N}$, vem: $g(a+d) = g(b+c)$. Como $g \in \mathbb{N}^*$, segue do cancelamento multiplicativo em $\mathbb{N}$ que $a+d = b+c$, ou seja, $\overline{(a,b)} = \overline{(c,d)}$. Ou, como queríamos, $\alpha = \beta$. □

Exercício 47. Mostre que $\overline{(0,0)} \cdot \alpha = \overline{(0,0)}$, para todo $\alpha \in \mathbb{Z}$.

Exercício 48. Mostre que se $\alpha, \beta \in \mathbb{Z}$ e $\alpha\beta = \overline{(0,0)}$, então $\alpha = \overline{(0,0)}$ ou $\beta = \overline{(0,0)}$. (Sugestão: use o exercício anterior e o cancelamento multiplicativo.)

Exercício 49. Mostre que se $\alpha, \beta \in \mathbb{Z}$, então $(-\alpha)\beta = -\alpha\beta = \alpha(-\beta)$ e $(-\alpha)(-\beta) = \alpha\beta$.

Exercício 50. Demonstre a *propriedade distributiva da multiplicação em relação à subtração*: $\alpha \cdot (\beta - \gamma) = \alpha \cdot \beta - \alpha \cdot \gamma$.

3.3 Relação de ordem em $\mathbb{Z}$

Como em $\mathbb{N}$, vamos comparar os elementos de $\mathbb{Z}$ através de uma relação de ordem.

Com motivações análogas àquelas que precederam as definições de adição e de multiplicação, temos a seguinte definição:

Definição 3.3.1. Dados os inteiros $\overline{(a,b)}$ e $\overline{(c,d)}$, escrevemos $\overline{(a,b)} \leq \overline{(c,d)}$ (lê-se $\overline{(a,b)}$ *é menor do que ou igual a* $\overline{(c,d)}$), quando $a+d \leq b+c$.

Os símbolos $\geq$, $>$ e $<$ definem-se de forma análoga à que fizemos para a relação de ordem em $\mathbb{N}$.

Como nos casos da adição e da multiplicação, verifica-se que a relação que acabamos de introduzir está bem definida. Certifique-se desse fato. Os símbolos de

desigualdade utilizados para a relação de ordem em $\mathbb{Z}$ são os mesmos que utilizamos para a relação de ordem em $\mathbb{N}$, mas o contexto deixará claro que ordem está sendo considerada. Além disso, o Teorema 3.3.2 adiante nos mostrará que esta diferença de contextos é provisória, uma vez que a ordem em $\mathbb{Z}$ será uma *extensão* da ordem em $\mathbb{N}$.

Teorema 3.3.1. *A relação $\leq$ definida acima é uma relação de ordem em $\mathbb{Z}$, ou seja, é reflexiva, antissimétrica e transitiva. Além disso, essa relação é compatível com as operações em $\mathbb{Z}$, isto é, para $\alpha, \beta, \gamma \in \mathbb{Z}$ arbitrários, vale:*

i) $\alpha \leq \beta \Rightarrow \alpha + \gamma \leq \beta + \gamma$;

ii) $\alpha \leq \beta$ *e* $\gamma \geq \overline{(0,0)} \Rightarrow \alpha\gamma \leq \beta\gamma$.

iii) (Lei da Tricotomia): Apenas uma das situações seguintes ocorre:
$\alpha = \overline{(0,0)}$ *ou* $\alpha < \overline{(0,0)}$ *ou* $\alpha > \overline{(0,0)}$.

Demonstração. O leitor deve demonstrar como exercício que $\leq$ é uma relação de ordem, bem como os itens (i) e (iii) . Demonstraremos (ii):

Ponhamos $\alpha = \overline{(a,b)}$, $\beta = \overline{(c,d)}$ e $\gamma = \overline{(e,f)}$.

A hipótese se reescreve: $a + d \leq b + c$ e $f \leq e$.

Logo, existem $p, q \in \mathbb{N}$ tais que

$$b + c = a + d + p \tag{3.3}$$

e

$$e = f + q \tag{3.4}$$

De (3.3), obtemos:

$$be+ce = ae+de+pe \text{ e } bf+cf = af+df+pf.$$

Segue que

$$ae+de+pe+bf+cf = af+df+pf+be+ce. \tag{3.5}$$

De (3.4), obtemos:

$$pe = pf+pq. \tag{3.6}$$

Assim, (3.6) em (3.5) fornece:

$$ae+de+pf+pq+bf+cf = af+df+pf+be+ce.$$

Segue daí que $ae+de+bf+cf \leq af+df+be+ce$, que equivale a $\alpha\gamma \leq \beta\gamma$. □

Exercício 51. Mostre que, para $\alpha, \beta \in \mathbb{Z}$, apenas uma das situações seguintes ocorre: $\alpha = \beta$ ou $\alpha < \beta$ ou $\alpha > \beta$.

Exercício 52. Mostre que se $\alpha, \beta \in \mathbb{Z}$, $\alpha \leq \beta$ e $\gamma < \overline{(0,0)}$, então $\alpha\gamma \geq \beta\gamma$.

Definição 3.3.2. Dado $\overline{(a,b)} \in \mathbb{Z}$, dizemos que:

i) $\overline{(a,b)}$ é *positivo* quando $\overline{(a,b)} > \overline{(0,0)}$;

ii) $\overline{(a,b)}$ é *não negativo* quando $\overline{(a,b)} \geq \overline{(0,0)}$;

iii) $\overline{(a,b)}$ é *negativo* quando $\overline{(a,b)} < \overline{(0,0)}$;

iv) $\overline{(a,b)}$ é *não positivo* quando $\overline{(a,b)} \leq \overline{(0,0)}$.

Observe que $\overline{(a,b)} \geq \overline{(0,0)}$ significa $a+0 \geq b+0$, isto é, $a \geq b$.

Analogamente, temos:

$\overline{(a,b)} > \overline{(0,0)} \Leftrightarrow a > b$, $\overline{(a,b)} \leq \overline{(0,0)} \Leftrightarrow a \leq b$ e $\overline{(a,b)} < \overline{(0,0)} \Leftrightarrow a < b$.

Essa observação está de acordo com a ideia de que a classe de equivalência $\overline{(a,b)}$ representa a "diferença $a-b$". Tornaremos essa ideia precisa mais adiante, ao final das observações após o próximo teorema.

Observe ainda que se $\overline{(a,b)}$ é positivo, como $a > b$, então existe $m \in \mathbb{N}^*$ tal que $a = b + m$. Esta igualdade equivale a $\overline{(a,b)} = \overline{(m,0)}$. Analogamente, se $\overline{(a,b)} < \overline{(0,0)}$, então existe $m \in \mathbb{N}^*$ tal que $\overline{(a,b)} = \overline{(0,m)}$.

Essas observações e a tricotomia em $\mathbb{Z}$ nos dizem que:

$$\mathbb{Z} = \{\overline{(0,m)} \mid m \in \mathbb{N}^*\} \cup \{\overline{(0,0)}\} \cup \{\overline{(m,0)} \mid m \in \mathbb{N}^*\},$$

sendo a união disjunta.

Utilizaremos as seguintes notações (conforme início da Seção 1.2):

$$\mathbb{Z}_-^* = \{\overline{(0,m)} \mid m \in \mathbb{N}^*\}, \quad \mathbb{Z}_- = \mathbb{Z}_-^* \cup \{\overline{(0,0)}\},$$
$$\mathbb{Z}_+^* = \{\overline{(m,0)} \mid m \in \mathbb{N}^*\} \text{ e } \mathbb{Z}_+ = \mathbb{Z}_+^* \cup \{\overline{(0,0)}\}.$$

Note ainda que o conjunto dos números inteiros não negativos, $\mathbb{Z}_+$, está em bijeção com $\mathbb{N}$. Esta bijeção é bastante especial porque mostra que $\mathbb{Z}_+$ é uma "*cópia algébrica*" de $\mathbb{N}$, no sentido dado pelo teorema seguinte.

Teorema 3.3.2. *Seja $f : \mathbb{N} \to \mathbb{Z}$ dada por $f(m) = \overline{(m,0)}$. Então f é injetora e valem as seguintes propriedades:*

i) $f(m+n) = f(m) + f(n)$;

ii) $f(mn) = f(m) \cdot f(n)$;

iii) Se $m \leq n$, então $f(m) \leq f(n)$.

Exercício 53. Demonstre o teorema acima.

O conjunto $f(\mathbb{N}) = \mathbb{Z}_+$ tem, pelo teorema acima, a mesma estrutura algébrica que $\mathbb{N}$. Por exemplo: $3+5=8$, em $\mathbb{N}$, corresponde, via f, a $\overline{(3,0)}+\overline{(5,0)} = \overline{(8,0)}$ em $\mathbb{Z}$. Do mesmo modo, $3\cdot 5 = 15$ corresponde, via f, a $\overline{(3,0)}\cdot\overline{(5,0)} = \overline{(15,0)}$. Finalmente, a relação $3 \leq 5$ se preserva, via f, como $\overline{(3,0)} \leq \overline{(5,0)}$, o que confirma nosso comentário do início desta seção de que a ordem em $\mathbb{Z}$ é uma *extensão* da ordem em $\mathbb{N}$.

Assim, do ponto de vista das operações aritméticas e da ordenação, $\mathbb{Z}_+$ é indistinguível de $\mathbb{N}$. Embora, no nosso contexto, $\mathbb{N}$ não seja um subconjunto de $\mathbb{Z}$, sua cópia algébrica $\mathbb{Z}_+$ o é.

A função $f : \mathbb{N} \to \mathbb{Z}$ acima chama-se *imersão* de $\mathbb{N}$ em $\mathbb{Z}$. Esta imersão mostra ainda que $\mathbb{Z}$ é infinito, conforme já comentado no Capítulo 2.

Observe ainda que, se $m \in \mathbb{N}$, o simétrico de $\overline{(m,0)}$ é $\overline{(0,m)}$. Logo, se identificarmos $\overline{(m,0)}$ com m através de f, obtemos: $-m = -\overline{(m,0)} = \overline{(0,m)}$.

Obtemos então, sob a identificação de $\mathbb{N}$ com $\mathbb{Z}_+$, via f, que:

$$\mathbb{Z} = \{-m \mid m \in \mathbb{N}^*\} \cup \{0\} \cup \mathbb{N}^* = \{\ldots,-m,\ldots,-2,-1,0,1,2,\ldots,m,\ldots\},$$

como no Ensino Fundamental.

A partir de agora, passaremos a adotar esta identificação e, então, considerar $\mathbb{N}$ um subconjunto de $\mathbb{Z}$. Sob tal identificação, obtemos:

$$a-b = \overline{(a,0)} - \overline{(b,0)} = \overline{(a,0)} + (-\overline{(b,0)}) = \overline{(a,0)} + (\overline{(0,b)}) = \overline{(a,b)},$$

conforme anunciado no início deste capítulo.

Exercício 54. Efetue em $\mathbb{Z}$:

1) $3-5$; 2) $8-13$; 3) $13-8$; 4) $3-(-5)$; 5) $-3+(-5)$;
6) $3\cdot 5$; 7) $(-3)\cdot 5$; 8) $3\cdot(-5)$; 9) $(-3)\cdot(-5)$.

Exercício 55. Mostre que, para $x, y \in \mathbb{Z}$, temos:

1. se $x > 0$ e $y > 0$, então $xy > 0$;

2. se $x < 0$ e $y < 0$, então $xy > 0$;

3. se $x < 0$ e $y > 0$ então $xy < 0$.

Exercício 56. Mostre que os itens (*i*) e (*ii*) do Teorema 3.3.1 continuam válidos com a relação "$<$" no lugar de "$\leq$" (e $\gamma > 0$ no caso (*ii*)).

Mostraremos a seguir, à semelhança de $\mathbb{N}$, que o conjunto $\mathbb{Z}$ é bem ordenado. Antes, porém, algumas definições.

Definição 3.3.3. Seja X um subconjunto não vazio de $\mathbb{Z}$. Dizemos que X é *limitado inferiormente* se existe $\alpha \in \mathbb{Z}$ tal que $\alpha \leq x$, para todo $x \in X$. Um tal α se chama *cota inferior de* X. Analogamente, definimos subconjunto de $\mathbb{Z}$ *limitado superiormente* e *cota superior* dele.

Exemplo 3.3.1. O elemento 0 é cota inferior para $\mathbb{N} \subset \mathbb{Z}$. Da mesma forma, -1 o é, bem como qualquer inteiro negativo.

Exercício 57. Mostre que $\mathbb{N}$ não admite cota superior em $\mathbb{Z}$.

Teorema 3.3.3. *(Princípio da Boa Ordem para $\mathbb{Z}$) Seja $X \subset \mathbb{Z}$ não vazio e limitado inferiormente. Então X possui elemento mínimo.*

Demonstração. Seja α uma cota inferior de X, isto é, $\alpha \leq x$, $\forall x \in X$.

Considere o conjunto $X' = \{x - \alpha \mid x \in X\}$. Claramente, $X' \subset \mathbb{N}$ (identificado com $\mathbb{Z}_+$) e, pelo Princípio da Boa Ordem em $\mathbb{N}$, o conjunto X' possui elemento mínimo, digamos, m'.

Assim, $m' \in X'$ e $m' \leq y$, $\forall y \in X'$. Como $m' \in X'$, m' é da forma $m - \alpha$, para algum $m \in X$. Afirmamos que $m = m' + \alpha$ é elemento mínimo de X. Só falta verificar que $m \leq x$, $\forall x \in X$, mas isso equivale a $m - \alpha \leq x - \alpha$, $\forall x \in X$, ou seja, $m' \leq y$, $\forall y \in X'$, que é verdade pela definição de m'. Logo, m é o elemento mínimo de X. □

Corolário 3.3.4. *Seja $x \in \mathbb{Z}$ tal que $0 < x \leq 1$. Então $x = 1$.*

Demonstração. Seja $A = \{y \in \mathbb{Z} \mid 0 < y \leq 1\}$. Tem-se:

$A \neq \emptyset$ (pois $1 \in A$) e A é limitado inferiormente por 0. Pelo Princípio da Boa Ordem, A possui elemento mínimo, digamos, m. Suponhamos que $m < 1$. Assim $0 < m < 1$, de onde segue que $0 < m^2 < m < 1$, o que implica $m^2 \in A$, contrariando a minimalidade de m.

Assim, $m = 1$ e $A = \{1\}$. □

Corolário 3.3.5. *Sejam $n, x \in \mathbb{Z}$ tais que $n < x \leq n+1$. Então $x = n+1$.*

Exercício 58. Prove o Corolário 3.3.5.

Compare o teorema acima e seus corolários com seus correspondentes em $\mathbb{N}$: Teorema 2.3.4 e Teorema 2.3.5.

Para finalizar esta seção, vamos definir o conceito de *módulo* ou *valor absoluto* de um número inteiro.

Definição 3.3.4. Seja $x \in \mathbb{Z}$. Definimos o *valor absoluto de x* (ou *módulo* de x), denotado por $|x|$, como sendo:

$$|x| = \begin{cases} x, & \text{se} \quad x \geq 0; \\ -x, & \text{se} \quad x < 0. \end{cases}$$

Exemplo 3.3.2. $|-3| = |3| = 3$; $|0| = 0$.

Exercício 59. Mostre que:

1) Mostre que $|x| \geq 0$, $\forall x \in \mathbb{Z}$ e que $|x| = 0$ se, e somente se, $x = 0$.

2) $|xy| = |x||y|$, $\forall x, y \in \mathbb{Z}$.

3) Para $n \in \mathbb{N}^*$, tem-se: $|x| = n$ se, e somente se, $x = n$ ou $x = -n$.

Definição 3.3.5. Um elemento $x \in \mathbb{Z}$ diz-se *inversível* se existe $y \in \mathbb{Z}$ tal que $xy = 1$ (conforme definição geral dada no Exercício 39).

Note que o elemento 0 não é inversível em $\mathbb{Z}$.

Proposição 3.3.6. *Os únicos elementos inversíveis de $\mathbb{Z}$ são 1 e -1.*

Demonstração. Seja $x \in \mathbb{Z}^*$ inversível e $y \in \mathbb{Z}$ tal que $xy = 1$. Segue que $1 = |xy| = |x||y|$. Como $|x| \geq 0$, $|y| \geq 0$ e $|x||y| = 1$, então $|x| > 0$ e $|y| > 0$, e daí resulta que, $|x| \geq 1$ e $|y| \geq 1$. Multiplicando ambos os membros da última desigualdade por $|x|$, obtemos:

$$1 = |x||y| \geq |x| \geq 1,$$

de onde segue que $|x| = 1$. Portanto, $x = 1$ ou $x = -1$, como queríamos provar. □

3.4 Conjuntos enumeráveis e a Hipótese do Contínuo

Exercício 60. Exiba duas funções injetoras de $\mathbb{N}$ em $\mathbb{Z}$ diferentes da imersão.

O exercício seguinte exibe uma bijeção entre $\mathbb{N}$ e $\mathbb{Z}$, o que fornece uma outra demonstração, via definição de Cantor (conforme Seção 2.1), de que $\mathbb{Z}$ é infinito.

Exercício 61. Mostre que é bijetora a função $\sigma\colon \mathbb{Z} \to \mathbb{N}$ definida como segue:

$$\sigma(n) = \begin{cases} 2n-1, & \text{se } n > 0 \\ -2n, & \text{se } n \leq 0 \end{cases}$$

Os conjuntos para os quais existe uma bijeção entre eles e $\mathbb{N}$ são notáveis em matemática e são denominados *conjuntos enumeráveis*. Qualquer bijeção de $\mathbb{N}$ em um conjunto enumerável A chama-se uma *enumeração* para A, segundo a qual o primeiro elemento de A é a imagem do 1, o segundo é a imagem do 2, e assim por diante (a imagem do 0 é o *zero-ésimo elemento de* A.). Assim, o exercício acima nos diz que $\mathbb{Z}$ é enumerável e apresenta a inversa da bijeção σ como uma enumeração para $\mathbb{Z}$. Mostraremos nos capítulos seguintes que $\mathbb{Q}$, surpreendentemente, também é enumerável, mas $\mathbb{R}$ e $\mathbb{C}$ não o são.

Exercício 62. Explicite a enumeração $\sigma^{-1} : \mathbb{N} \to \mathbb{Z}$ para $\mathbb{Z}$, onde σ é a bijeção do exercício anterior. Qual é o quinto número inteiro segundo essa enumeração? E o décimo? E o elemento de ordem 483?

Exercício 63. Mostre que não há uma enumeração $\alpha : \mathbb{N} \to \mathbb{Z}$, para $\mathbb{Z}$, que respeite a relação de ordem em $\mathbb{Z}$.

Como vimos no Capítulo 2, Cantor rompeu com o paradigma grego de que "o todo é sempre maior do que qualquer uma de suas partes próprias", exatamente ao caracterizar conjuntos infinitos como aqueles que podem ser colocados em bijeção com uma parte própria sua. Por outro lado, seus estudos generalizaram para conjuntos infinitos o fato elementar conhecido para conjuntos finitos de que o número de elementos de um conjunto é sempre menor do que o número de elementos das

partes desse conjunto. Dado um conjunto finito X, denotamos por $\eta(X)$ o número de elementos de X, conforme definido na seção 2.1.

Exercício 64. Mostre, usando indução (ou algum argumento de contagem), que se $\eta(X) = n$, então $\eta(\mathcal{P}(X)) = 2^n$.

Cantor generalizou para conjuntos infinitos a proposição contida no exercício acima ao provar que se X é infinito, então nenhuma função injetora de X em $\mathcal{P}(X)$ poderá ser sobrejetora (veja o último teorema deste capítulo). Uma injeção bastante natural de X em $\mathcal{P}(X)$ é $x \mapsto \{x\}$. Intuitivamente, o tipo de infinito de $\mathcal{P}(X)$ é estritamente maior do que o tipo de infinito de X. Expressamos esse fato dizendo que a *cardinalidade de* $\mathcal{P}(X)$ *é maior do que a cardinalidade de* X. Tomando agora $\mathcal{P}(\mathcal{P}(X))$ e denotando ainda por $\eta(X)$ a cardinalidade do conjunto infinito X, que é, grosso modo, o *tipo de infinito de* X, obtemos que $\eta(\mathcal{P}(X)) < \eta(\mathcal{P}(\mathcal{P}(X)))$. Continuando tomando partes de conjuntos das partes sucessivamente, chegamos aos infinitos tipos de infinito de Cantor (na verdade, esse processo nos dá uma quantidade enumerável de cardinalidades). Cantor debruçou-se sobre essas questões, tornando-as rigorosas matematicamente através de sua *aritmética transfinita*, estudada nos bons textossobre Teoria dos Conjuntos, como [17] e [30].

Vale a pena aqui mencionar um pequeno trecho sobre o trabalho de Cantor, que adaptamos da excelente referência sobre História da Matemática [27]:

"O grandioso e inovador trabalho de Cantor, para a consolidação dos fundamentos da matemática, fora desprezado, por anos, por grande parte da comunidade matemática da época, especialmente pela influência negativa de Leopold Kronecker, um dos antigos professores de Cantor na Universidade de Berlim. Cantor conseguiu publicar seu primeiro grande artigo sobre sua Teoria dos Conjuntos após meses da

data de sua aprovação. O atraso se deu deliberadamente por Kronecker, um dos editores do jornal ao qual Cantor submeteu o artigo. Esse atraso deveu-se à censura acadêmica e, principalmente, à inveja profissional do velho professor. É de Kronecker a famosa frase - *Deus fez os naturais; o resto é coisa dos homens* -, na qual ele acreditava piamente. Para Kronecker, números negativos, frações, números complexos imaginários e, especialmente, números irracionais, eram a fonte de toda a desarmonia em matemática, o que reflete, obviamente, uma visão diametralmente oposta à de Cantor. Kronecker usou sua influência e posição acadêmica superior à de Cantor para abafar as 'heresias' cantorianas."

Consideremos agora a cadeia crescente de cardinalidades

$$\eta(\mathbb{N}) < \eta(\mathcal{P}(\mathbb{N})) < \eta(\mathcal{P}(\mathcal{P}(\mathbb{N}))) < \cdots.$$

Essa cadeia começa com a cardinalidade de $\mathbb{N}$ que, pela Definição 2.1.1 de conjunto infinito, pode ser considerada a menor cardinalidade infinita.

Uma pergunta natural é a seguinte: há cardinalidades intermediárias entre duas consecutivas dessa cadeia? Curiosamente, o fato é que não se tem resposta a essa pergunta, no seguinte sentido: não há como provar que a resposta é afirmativa ou negativa com base nos fundamentos da matemática dados pela *Teoria dos Conjuntos de Zermelo-Fraenkel*. Isso foi estabelecido pelo matemático americano Paul J. Cohen (1934-2007). A suposição de que a resposta é negativa denomina-se *Hipótese Generalizada do Contínuo*. O matemático austríaco naturalizado americano Kurt Gödel (1906-1978) provou que a Hipótese Generalizada do Contínuo não é contraditória com os outros axiomas da Teoria dos Conjuntos (de Zermelo-Fraenkel), o que quer dizer que não obtemos contradições extras na matemática obtida ao adicionar a Hipótese Generalizada do Contínuo aos demais axiomas da Teoria dos Conjuntos.

O termo "Generalizada", na expressão acima, deve-se ao fato de que a *Hipótese do Contínuo* (sem o termo "Generalizada") diz respeito à primeira desigualdade na cadeia acima. Trata-se da suposição de que não há cardinalidades intermediárias entre a de $\mathbb{N}$ e a de $\mathcal{P}(\mathbb{N})$. Este caso particular é notável porque, como provaremos no Capítulo 5, $\eta(\mathbb{R}) > \eta(\mathbb{N})$, o que diz ser $\mathbb{R}$ não enumerável. Além disso, provaremos na Proposição 5.4 que $\eta(\mathbb{R}) = \eta(\mathcal{P}(\mathbb{N}))$, ou seja, $\mathbb{R}$ e $\mathcal{P}(\mathbb{N})$ são equipotentes. (Veja, por exemplo, [30] ou [17] para maiores considerações sobre a Teoria dos Conjuntos e a aritmética transfinita de Cantor.)

Assim, assumindo a Hipótese do Contínuo, concluímos que, no imenso e matematicamente rico universo existente entre $\mathbb{N}$ e $\mathbb{R}$, onde, como veremos, moram os números racionais, irracionais, transcendentes e algébricos reais, não são obtidas cardinalidades distintas das desses dois conjuntos, isto é, qualquer subconjunto infinito de $\mathbb{R}$, ou é equipotente a $\mathbb{N}$ (enumerável), ou é equipotente a $\mathbb{R}$.

Para concluir este capítulo, vamos demonstrar o teorema de Cantor que, em certo sentido, generaliza o Exercício 3.4, como havíamos comentado.

Teorema 3.4.1. *Seja X um conjunto não vazio qualquer. Nenhuma função $f : X \longrightarrow \mathcal{P}(X)$ pode ser sobrejetora.*

Demonstração. Para cada $x \in X$, $f(x)$ é um subconjunto de X. Seja $A = \{x \in X \mid x \notin f(x)\}$. Mostraremos que $A \notin Im(f)$. Suponhamos o contrário, isto é, que existe $a \in X$ tal que $f(a) = A$. Agora, ou $a \in A$ ou $a \in X \setminus A$. No primeiro caso, pela definição de A, devemos ter $a \notin f(a)$. Mas $f(a) = A$, uma contradição. No segundo caso, devemos ter $a \in f(a) = A$, outra contradição. Segue, então, que $A \notin Im(f)$. □

4

Números racionais

No Ensino Fundamental, aprendemos que um número racional é a "razão" entre dois números inteiros. Assim, por exemplo, o número $\frac{3}{5}$ é a "razão" entre 3 e 5. O termo "razão" naquele contexto significa "divisão". Dessa forma, $\frac{3}{5}$ é o mesmo que $3:5$, que tem o mesmo resultado que a divisão $6:10$, o qual se escreve como $0,6$.

No nosso contexto, os termos "razão", "divisão" e mesmo "fração" devem ser definidos com base no que já temos, isto é, o conjunto dos números inteiros e suas propriedades algébricas. Notemos que em $\mathbb{Z}$ estão definidas apenas as operações de adição, de multiplicação e a subtração, que é um caso particular da adição: $a-b$ é, por definição, $a+(-b)$, onde $-b$ é o simétrico de b.

Poderíamos tentar definir a divisão de modo análogo à definição de subtração, ou seja, $a:b=a.b^{-1}$, onde b^{-1} é o inverso multiplicativo de b, isto é, o número que multiplicado por b resulta no neutro multiplicativo 1 (do mesmo modo que o simétrico de b é o número $-b$, que somado a b resulta no neutro aditivo 0). O problema é que os únicos elementos inversíveis de $\mathbb{Z}$ são o 1 e o -1, conforme a Proposição 3.3.6, logo, não faz sentido a definição de divisão acima, dentro dos propósitos de uma definição rigorosa de número racional.

Para chegarmos à tal definição, novamente trabalharemos com o conceito de relação de equivalência, do mesmo modo que o utilizamos para definir um número inteiro a partir do conceito de número natural. Acompanhe a semelhança do desenvolvimento a seguir com o realizado na construção de $\mathbb{Z}$ a partir de $\mathbb{N}$.

4.1 Construção dos números racionais

Consideremos o conjunto $\mathbb{Z} \times \mathbb{Z}^* = \{(a,b) \mid a \in \mathbb{Z} \text{ e } b \in \mathbb{Z}^*\}$. Definamos nele a relação: $(a,b) \sim (c,d)$ quando $ad = bc$.

Teorema 4.1.1. *A relação acima é de equivalência.*

Demonstração. A prova de que $\sim$ tem as propriedades reflexiva e simétrica fica como exercício. Quanto à propriedade transitiva, se $(a,b) \sim (c,d)$ e $(c,d) \sim (e,f)$, então queremos mostrar que $(a,b) \sim (e,f)$, isto é, se $ad = bc$ e $cf = de$, então $af = be$. Multiplicando ambos os membros da primeira igualdade acima por f e da segunda igualdade por b, obtemos $adf = bcf$ e $bcf = bde$, de onde segue que $adf = bde$. Cancelando o fator $d \neq 0$, obtemos o que queríamos. □

É por causa deste último detalhe da demonstração que partimos de $\mathbb{Z} \times \mathbb{Z}^*$ e não de $\mathbb{Z} \times \mathbb{Z}$.

Exercício 65. Faça uma observação análoga à feita após o Teorema 3.1.1 para entender a motivação do ponto de partida para a construção de $\mathbb{Q}$.

Exemplo 4.1.1. Temos:

a) $(1,2) \sim (2,4) \sim (-31,-62)$; b) $(5,1) \sim (-10,-2)$.

Definição 4.1.1. Dado $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$, denotamos por $\frac{a}{b}$ (que se lê "*a sobre b*") a classe de equivalência do par (a,b) pela relação $\sim$ acima. Assim,

$$\frac{a}{b} = \{(x,y) \in \mathbb{Z} \times \mathbb{Z}^* \mid (x,y) \sim (a,b)\}.$$

Exemplo 4.1.2. $\frac{1}{2} = \{(x,y) \in \mathbb{Z} \times \mathbb{Z}^* \mid (x,y) \sim (1,2)\} = \{(x,y) \in \mathbb{Z} \times \mathbb{Z}^* \mid 2x = y\}$.
Assim, temos: $(1,2) \in \frac{1}{2}$; $(-31,-62) \in \frac{1}{2}$; $(2,5) \notin \frac{1}{2}$.

Exemplo 4.1.3. $\frac{5}{1} = \{(x,y) \in \mathbb{Z} \times \mathbb{Z}^* \mid (x,y) \sim (5,1)\} = \{(x,y) \in \mathbb{Z} \times \mathbb{Z}^* \mid x = 5y\}$.
Logo, obtemos: $(5,1) \in \frac{5}{1}$; $(-10,-2) \in \frac{5}{1}$; $(2,5) \notin \frac{5}{1}$.

Teorema 4.1.2. *(Propriedade fundamental das frações) Se* (a,b) *e* (c,d) *são elementos de* $\mathbb{Z} \times \mathbb{Z}^*$, *então* $\frac{a}{b} = \frac{c}{d}$ *se, e somente se,* $ad = bc$.

Demonstração. Temos, pelo Teorema 1.2.2 - (ii):

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow (a,b) \sim (c,d) \Leftrightarrow ad = bc,$$

provando o resultado. □

Temos agora um significado preciso para o símbolo de *fração* $\frac{a}{b}$. Trata-se de uma classe de equivalência com respeito à relação de equivalência que acabamos de introduzir.

Definição 4.1.2. Denotamos por $\mathbb{Q}$, e denominamos *conjunto dos números racionais*, o conjunto quociente de $\mathbb{Z} \times \mathbb{Z}^*$ pela relação de equivalência $\sim$, isto é,

$$\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}^*)/\sim\, = \left\{\frac{a}{b} \mid a \in \mathbb{Z} \text{ e } b \in \mathbb{Z}^*\right\},$$

como no Ensino Fundamental.

4.2 Operações em $\mathbb{Q}$

Vamos agora definir duas operações em $\mathbb{Q}$, dotando-o, portanto, de uma estrutura algébrica que estudaremos posteriormente. No Ensino Fundamental aprendemos que $\mathbb{Z} \subset \mathbb{Q}$. É claro que do nosso ponto de vista atual isso não faz sentido, pois os elementos de $\mathbb{Q}$ são classes de equivalência de pares de inteiros, logo de natureza diferente da dos números inteiros. No entanto, veremos que existe uma aplicação injetora de $\mathbb{Z}$ em $\mathbb{Q}$ que "preserva" as operações aritméticas e, dessa forma, permite que a imagem de $\mathbb{Z}$ em $\mathbb{Q}$ por essa aplicação seja uma *cópia algébrica* de $\mathbb{Z}$ em $\mathbb{Q}$. Assim, do ponto de vista da álgebra, poderemos considerar $\mathbb{Z}$ como um subconjunto de $\mathbb{Q}$. Note a analogia com a imersão de $\mathbb{N}$ em $\mathbb{Z}$.

A definição a seguir tem motivações análogas àquelas dadas para definir as operações em $\mathbb{Z}$ e o leitor é convidado a investigá-las.

Definição 4.2.1. Sejam $\frac{a}{b}$ e $\frac{c}{d}$ números racionais, isto é, elementos de $\mathbb{Q}$. Definimos as operações chamadas de *adição* e de *multiplicação*, respectivamente, por:

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd} \quad e \quad \frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}.$$

Denotaremos $\frac{a}{b}\cdot\frac{c}{d}$ também por $\frac{a}{b}\,\frac{c}{d}$.

Exemplo 4.2.1. Temos:

1) $\frac{1}{2}+\frac{5}{3}=\frac{1\cdot 3+2\cdot 5}{2\cdot 3}=\frac{13}{6}$.

2) $\frac{1}{2}\cdot\frac{5}{3}=\frac{1\cdot 5}{2\cdot 3}=\frac{5}{6}$.

3) $\dfrac{2}{4}+\dfrac{5}{3}=\dfrac{2\cdot 3+4\cdot 5}{4\cdot 3}=\dfrac{26}{12}=\dfrac{13}{6}.$

4) $\dfrac{2}{4}\cdot\dfrac{5}{3}=\dfrac{2\cdot 5}{4\cdot 3}=\dfrac{10}{12}=\dfrac{5}{6}.$

Note que obtivemos os mesmos resultados nos dois pares de exemplos acima, o que não deve causar surpresa, pois $\frac{2}{4}=\frac{1}{2}$, pelo Teorema 4.1.2. Entretanto, devemos verificar que as definições acima mantêm sempre esta coerência, isto é, se $\frac{a}{b}=\frac{a'}{b'}$ e $\frac{c}{d}=\frac{c'}{d'}$, então $\frac{a}{b}+\frac{c}{d}=\frac{a'}{b'}+\frac{c'}{d'}$ e $\frac{a}{b}\cdot\frac{c}{d}=\frac{a'}{b'}\cdot\frac{c'}{d'}$.

Isso se expressa nos termos do teorema seguinte.

Teorema 4.2.1. *As operações em* $\mathbb{Q}$*, acima, estão bem definidas.*

Demonstração. Temos, por hipótese, que $ab'=ba'$ e $cd'=dc'$. Faremos a demonstração referente à adição e deixaremos como exercício para o leitor a referente à multiplicação.

Temos:

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd},\qquad \frac{a'}{b'}+\frac{c'}{d'}=\frac{a'd'+b'c'}{b'd'}.$$

Queremos provar que as duas somas são iguais, ou seja, que $(ad+bc)b'd'=(a'd'+b'c')bd$, isto é, $adb'd'+bcb'd'=a'd'bd+b'c'bd$, ou, $(ab')(dd')+(bb')(cd')=(a'b)(dd')+(bb')(c'd)$, o que segue imediatamente da hipótese acima. □

Teorema 4.2.2. *O conjunto $\mathbb{Q}$, munido das operações acima, tem as propriedades algébricas de $\mathbb{Z}$, onde o elemento neutro aditivo é $\frac{0}{1}$ e o neutro multiplicativo é $\frac{1}{1}$. Além disso, dado um racional $\frac{a}{b} \neq \frac{0}{1}$, existe $\frac{c}{d}$ em $\mathbb{Q}$ tal que $\frac{a}{b} \cdot \frac{c}{d} = \frac{1}{1}$, isto é, todo elemento não nulo de $\mathbb{Q}$ (ou seja, diferente do neutro aditivo $\frac{0}{1}$) possui inverso multiplicativo.*

Demonstração. Devemos mostrar que, para elementos arbitrários $r, s, t \in \mathbb{Q}$, vale:

1. $r + s = s + r$;
2. $(r+s)+t = r+(s+t)$;
3. $r + \frac{0}{1} = r$;
4. Existe r' tal que $r + r' = \frac{0}{1}$;
5. $rs = sr$;
6. $(rs)t = r(st)$;
7. $r \cdot \frac{1}{1} = r$;
8. Se $r \neq \frac{0}{1}$, existe r'' tal que $rr'' = \frac{1}{1}$;
9. $r(s+t) = rs + rt$.

Mostraremos apenas (1). A demonstração dos demais itens é um exercício para o leitor.

Sejam $r = \frac{a}{b}$ e $s = \frac{c}{d}$, onde $a, c \in \mathbb{Z}$ e $b, d \in \mathbb{Z}^*$. Temos:

$$r + s = \frac{ad + bc}{bd} \quad e \quad s + r = \frac{cb + da}{db}.$$

A igualdade $r+s=s+r$ segue então da comutatividade da adição e da multiplicação em $\mathbb{Z}$. □

Os elementos r' e r'' tais que $r+r'=\frac{0}{1}$ e $rr''=\frac{1}{1}$ são únicos (lembre o Exercício 39) e denotam-se por $-r$ e r^{-1}, chamados de simétrico e inverso de r, respectivamente.

Exercício 66. Enuncie e demonstre uma proposição análoga à Proposição 3.2.3 para números racionais. Faça o mesmo para os Exercícios 49 e 50. Note que os fatos demonstrados nesses exercícios dependem apenas das propriedades das operações em $\mathbb{Z}$ e em $\mathbb{Q}$, logo são válidos em qualquer estrutura algébrica cujas operações possuem propriedades semelhantes às da adição e da multiplicação nesses dois conjuntos numéricos.

Exercício 67. Para $(a,b)\in\mathbb{Z}\times\mathbb{Z}^*$, mostre que: $\frac{-a}{b}=\frac{a}{-b}=-\frac{a}{b}=-\frac{-a}{-b}$.

Tendo em vista o exercício acima, podemos considerar que se $\frac{a}{b}\in\mathbb{Q}$, então b pode ser tomado positivo. Usaremos este fato para definir uma relação de ordem em $\mathbb{Q}$.

4.3 Relação de ordem e a enumerabilidade de $\mathbb{Q}$

Definição 4.3.1. Sejam $\frac{a}{b}$ e $\frac{c}{d}$ números racionais com $b,d>0$. Escrevemos $\frac{a}{b}\leq\frac{c}{d}$ quando $ad\leq bc$ e dizemos que $\frac{a}{b}$ é *menor do que ou igual* a $\frac{c}{d}$.

Vale aqui a observação notacional análoga àquela feita após a Definição 3.3.1.

Teorema 4.3.1. *A relação $\leq$, introduzida acima, está bem definida e é uma relação de ordem em $\mathbb{Q}$.*

Demonstração. Exercício. □

Exercício 68. (*Compatibilidade da ordem com as operações em* $\mathbb{Q}$) Mostre que, para $\alpha, \beta, \gamma \in \mathbb{Q}$, vale:

1. se $\alpha \leq \beta$, então $\alpha + \gamma \leq \beta + \gamma$;
2. se $\alpha \leq \beta$ e $\gamma \geq \frac{0}{1}$, então $\alpha\gamma \leq \beta\gamma$;
3. se $\alpha \leq \beta$ e $\gamma \leq \frac{0}{1}$, então $\alpha\gamma \geq \beta\gamma$.

Exercício 69. Mostre que, $\frac{a}{b} < \frac{c}{d} \iff a \cdot d < b \cdot c \ \ (b, d > 0)$.

Notação: como no caso de $\mathbb{Z}$, adotamos a notação: $\mathbb{Q}^*$, $\mathbb{Q}_-$, $\mathbb{Q}_+$, $\mathbb{Q}^*_-$ e $\mathbb{Q}^*_+$, com os significados usuais.

Teorema 4.3.2. *(Lei da Tricotomia em $\mathbb{Q}$) Dados $r, s \in \mathbb{Q}$, uma, e apenas uma, das situações seguintes ocorre: ou $r = s$, ou $r < s$, ou $s < r$.*

Demonstração. Escrevendo $r = \frac{a}{b}$ e $s = \frac{c}{d}$, com $b, d > 0$, comparemos os inteiros ad e bc. Pela Lei da Tricotomia em $\mathbb{Z}$, ou $ad = bc$, em cujo caso ocorre $r = s$, ou $ad < bc$, em cujo caso ocorre $r < s$, ou $ad > bc$, em cujo caso ocorre $s < r$. Além disso, a validade de uma das afirmações excluiu a validade das outras duas. □

Definamos agora uma função $i : \mathbb{Z} \to \mathbb{Q}$ por $i(n) = \frac{n}{1}$, para todo $n \in \mathbb{Z}$. Esta é a função de que falamos anteriormente, que "*imerge*" $\mathbb{Z}$ em $\mathbb{Q}$.

Teorema 4.3.3. *A função* $i : \mathbb{Z} \mapsto \mathbb{Q}$*, acima definida, é injetora. Além disso, ela preserva as operações e a relação de ordem de* $\mathbb{Z}$ *em* $\mathbb{Q}$ *no seguinte sentido:*

1. $i(m+n) = i(m) + i(n)$*;*

2. $i(mn) = i(m) \cdot i(n)$*;*

3. *se* $m \leq n$*, então* $i(m) \leq i(n)$.

Demonstração.

i) Mostremos que i é injetora: $i(n) = i(m) \Leftrightarrow \frac{n}{1} = \frac{m}{1} \Leftrightarrow n \cdot 1 = 1 \cdot m \Leftrightarrow n = m$.

ii) Mostremos que i preserva a estrutura algébrica de $\mathbb{Z}$:

$$i(n) + i(m) = \frac{n}{1} + \frac{m}{1} = \frac{1 \cdot n + m \cdot 1}{1 \cdot 1} = \frac{n+m}{1} = i(n+m);$$

$$i(n) \cdot i(m) = \frac{n}{1} \cdot \frac{m}{1} = \frac{n \cdot m}{1 \cdot 1} = \frac{nm}{1} = i(nm).$$

iii) Fica a cargo do leitor demonstrar que i preserva a relação de ordem. □

Assim, o conjunto $i(\mathbb{Z}) = \left\{ \frac{n}{1} \mid n \in \mathbb{Z} \right\}$ é uma cópia algébrica de $\mathbb{Z}$ em $\mathbb{Q}$. Essa imersão de $\mathbb{Z}$ em $\mathbb{Q}$ também mostra que $\mathbb{Q}$ é infinito, já que $\mathbb{Z}$ contém uma cópia de $\mathbb{N}$. Na verdade, $\mathbb{Q}$ é enumerável, e mostrar isso é o objetivo dos exercícios seguintes.

Exercício 70. Sejam X um subconjunto de um universo U e A_n, $n \in \mathbb{N}$, uma família de subconjuntos de U. Mostre que:

$$X \setminus (\bigcup_{n\in\mathbb{N}} A_n) = \bigcap_{n\in\mathbb{N}} (X \setminus A_n) \quad \text{e} \quad X \setminus (\bigcap_{n\in\mathbb{N}} A_n) = \bigcup_{n\in\mathbb{N}} (X \setminus A_n).$$

(Lembramos que $\bigcup_{n\in\mathbb{N}} A_n = \{x \in U \mid x \in A_n, \; para\ algum\ n \in \mathbb{N}\}$ e que $\bigcap_{n\in\mathbb{N}} A_n = \{x \in U \mid x \in A_n, \; para\ todo\ n \in \mathbb{N}\}$.)

Lema 4.3.4. *Todo subconjunto infinito de $\mathbb{N}$ é enumerável.*

Demonstração. Seja X um subconjunto infinito de $\mathbb{N}$ e x_0 seu menor elemento (que existe, devido ao Princípio da Boa Ordem). Como X é infinito, o conjunto $Y_0 = X \setminus \{x_0\}$ é não vazio. Seja agora x_1 o menor elemento de Y_0. Obtidos $x_0, x_1, x_2, ..., x_n$ ($n \in \mathbb{N}$) da forma acima, obtemos x_{n+1} como sendo o menor elemento de $Y_n = X \setminus \{x_0, x_1, x_2, ..., x_n\}$, que existe, pois Y_n é não vazio, para todo n natural, caso contrário, X seria finito (relembre as caracterizações de conjuntos finitos e infinitos mencionadas no Capítulo 2).

Afirmamos que
$X = \{x_0, x_1, x_2, ..., x_n, ...\} = \{x_0\} \bigcup \{x_0, x_1\} \bigcup \{x_0, x_1, x_2\} \bigcup ... = \bigcup_{n \in \mathbb{N}} A_n$,
onde $A_n = \{x_0, x_1, x_2, ..., x_n\}$. De fato, pelo exercício anterior, temos:
$X \setminus (\bigcup_{n \in \mathbb{N}} A_n) = \bigcap_{n \in \mathbb{N}} (X \setminus A_n) = \bigcap_{n \in \mathbb{N}} Y_n$. Assim, se existisse $x \in X \setminus (\bigcup_{n \in \mathbb{N}} A_n)$, esse x também seria elemento de $\bigcap_{n \in \mathbb{N}} Y_n$ e, como tal, deveria ser maior do que x_0, por estar em Y_0, deveria ser maior do que x_1 (que é maior do que x_0), por estar em Y_1 e, assim sucessivamente, x deveria ser maior do que x_n, para todo $n \in \mathbb{N}$. Dessa forma, o conjunto infinito $X = \{x_0, x_1, x_2, ..., x_n, ...\}$ estaria contido no conjunto finito $I_x = \{1, 2, 3, ..., x\}$ e seria, portanto, finito, uma contradição. □

No que segue, utilizaremos livremente o Teorema Fundamental da Aritmética, que pode ser demonstrado a partir das propriedades de $\mathbb{Z}$ que estudamos no capítulo anterior. Como mencionamos no Capítulo 1, esse teorema encontra-se exposto em vários itens da bibliografia. Ele diz essencialmente aquilo que já conhecemos intuitivamente desde o ensino básico de matemática. Seu enunciado é o seguinte: *todo número natural maior do que 1 pode ser expresso como produto de números*

primos. Além disso, essa fatoração é única, a menos da ordem dos fatores.

Lembremos ainda que *número natural primo* é todo número natural maior do que 1 que só admite como divisores os triviais: ele próprio e o 1.

Exercício 71. Expresse o número 60 como um produto de números naturais de várias formas distintas, sendo uma delas aquela dada pelo Teorema Fundamental da Aritmética.

Lema 4.3.5. *Todo número racional positivo* $\frac{a}{b}$, $(a,b > 0)$, *pode ser escrito, de modo único, como uma fração irredutível, isto é, na forma* $\frac{m}{n}$, *onde* m *e* n *são relativamente primos, isto é, não possuem fatores primos em comum.*

Demonstração. Considere as decomposições em fatores primos de a e de b, dadas pelo Teorema Fundamental da Aritmética. Seja k o produto de todos os fatores primos comuns a a e a b, de modo que $\frac{a}{b} = \frac{ka'}{kb'}$. Pela propriedade fundamental das frações, obtemos $\frac{a}{b} = \frac{a'}{b'}$, onde a' e b' são relativamente primos. Se houvesse uma fração irredutível $\frac{c}{d}$ igual a $\frac{a'}{b'}$, a propriedade fundamental das frações nos daria $a' \cdot d = b' \cdot c$, o que, pela unicidade da decomposição em fatores primos, obrigaria d a conter os fatores primos de b' e vice-versa, o mesmo ocorrendo para a' e c, ou seja, $a' = c$ e $b' = d$. □

Proposição 4.3.6. $\mathbb{Q}_+^*$ *é enumerável.*

Demonstração. Consideremos os números racionais escritos na forma irredutível, dada no Lema anterior. Seja $f : \mathbb{Q}_+^* \to \mathbb{N}$ dada por $f(\frac{m}{n}) = 2^m \cdot 3^n$. Novamente, o Teorema Fundamental da Aritmética e a unicidade da representação de frações na forma irredutível, dada pela proposição acima, mostram que f é injetora e tem

como imagem um subconjunto infinito de $\mathbb{N}$, que é, pelo Lema 4.3.4, enumerável. Daí segue o que queríamos provar. □

Exercício 72. Usando um argumento similar àquele empregado no Exercício 61, mostre que a união de dois conjuntos enumeráveis é enumerável. Conclua, usando indução, que a união de uma família finita de conjuntos enumeráveis é enumerável.

Exercício 73. Mostre que a união de um conjunto finito com um conjunto enumerável é enumerável.

Teorema 4.3.7. *$\mathbb{Q}$ é enumerável.*

Demonstração. Basta escrever $\mathbb{Q}$ como $\mathbb{Q}^*_- \bigcup \{0\} \bigcup \mathbb{Q}^*_+$ e aplicar os resultados acima. □

4.4 $\mathbb{Q}$ como corpo ordenado

O conjunto dos números racionais está munido das duas operações, adição e multiplicação, estudadas acima. Podemos definir a partir dessas operações, mais duas, a *subtração* e a *divisão*, simbolizadas por "$-$" e ":", respectivamente, da seguinte forma: se $r, s \in \mathbb{Q}$, define-se $r - s = r + (-s)$ (como em $\mathbb{Z}$) e, se $s \neq 0$, $r : s = r \cdot s^{-1}$. (Estritamente falando, a divisão não seria uma operação em $\mathbb{Q}$, uma vez que seu domínio não é $\mathbb{Q} \times \mathbb{Q}$, mas sim $\mathbb{Q} \times \mathbb{Q}^*$.)

Exercício 74. Mostre que se $a, b \in \mathbb{Z}$, com $b \neq 0$, então $\frac{a}{1} : \frac{b}{1} = \frac{a}{b}$. Assim, se identificarmos $\mathbb{Z}$ com sua cópia $i(\mathbb{Z})$ em $\mathbb{Q}$, a igualdade acima se escreve $a : b = \frac{a}{b}$. Compare com o que aprendemos no Ensino Fundamental.

Exercício 75. Mostre que se $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$, com $\frac{c}{d} \neq \frac{0}{1}$, então $\frac{a}{b} : \frac{c}{d} = \frac{ad}{bc}\cdot$ (É usual, nos textos elementares de matemática, adotar-se a notação $\frac{a/b}{c/d}$ para $\frac{a}{b} : \frac{c}{d}$, que estende a notação mencionada no exercício anterior.)

Exercício 76. Admitindo a identificação de $\mathbb{Z}$ com $i(\mathbb{Z})$ mostre que, para r, s racionais arbitrários, vale:

1. se $rs = 0$, então $s = 0$ ou $r = 0$;

2. se $r > 0$ e $s > 0$, então $rs > 0$;

3. se $r > 0$ e $s < 0$, então $rs < 0$;

4. se $r < 0$ e $s < 0$, então $rs > 0$;

5. se $r > 0$, então $r^{-1} > 0$;

6. se $r < s$, então $r < (r+s).2^{-1} < s$;

Exercício 77. Mostre que $\mathbb{Q}$ *não é bem ordenado*, isto é, existem em $\mathbb{Q}$ subconjuntos não vazios, limitados inferiormentes que não possuem elemento mínimo.

Apesar de $\mathbb{Q}$ não ser bem ordenado como $\mathbb{Z}$ (e $\mathbb{N}$), $\mathbb{Q}$ possui todas as propriedades aritméticas de $\mathbb{Z}$, além da propriedade de que todo elemento não nulo possui inverso, conforme o Teorema 4.2.2. Na linguagem algébrica, qualquer conjunto munido de duas operações, usualmente denotadas por $+$ e $\cdot$, com propriedades aritméticas análogas às de $\mathbb{Q}$, chama-se *corpo*. Se, além disso, um corpo estiver munido de uma relação de ordem compatível com suas operações aritméticas, ele é chamado

de *corpo ordenado*. Assim, $\mathbb{Q}$ é um exemplo de corpo ordenado. Há muitos exemplos de corpos, ordenados ou não ordenados, que são estudados em disciplinas da área de álgebra abstrata. Veremos nos capítulos seguintes que $\mathbb{R}$ e $\mathbb{C}$ são corpos, ordenado e não ordenado respectivamente.

Adotaremos a seguinte notação para os elementos de um corpo ordenado arbitrário K: continuaremos denotando por 0 e por 1 o neutro aditivo e o neutro multiplicativo de K, respectivamente, e, para a um natural maior do que 1, denotaremos também por a o elemento $1+1+\cdots+1$ (a vezes) de K. Assim, seu simétrico, $-a$, será $-(1+1+\cdots+1) = -1-1\cdots-1$. O contexto encarrega-se de deixar claro se o elemento 5, por exemplo, refere-se ao natural 5 ou ao $5 \in K$.

Exercício 78. Seja K um corpo ordenado, cujos elementos neutros aditivo e multiplicativo são respectivamente representados por 0 e 1 e a relação de ordem denotada por $\leq$. Mostre que:

1. se $0 = 1$, então K possui um só elemento;
2. $x^2 \geq 0$, para todo $x \in K$;
3. se $1 \neq 0$, então $1 > 0 > -1$;
4. se $1 \neq 0$, então K contém uma cópia de $\mathbb{N}$, de $\mathbb{Z}$ e de $\mathbb{Q}$ e é, portanto, infinito.

Exercício 79. Seja K como no exercício anterior, com $0 \neq 1$. Mostre que a aplicação $f : \mathbb{Q} \to K$ dada por $f(\frac{a}{b}) = a \cdot b^{-1}$, $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$, é uma imersão de $\mathbb{Q}$ em K que preserva a ordem, isto é, f tem as mesmas propriedades da imersão de $\mathbb{Z}$ em $\mathbb{Q}$ dadas pelo Teorema 4.3.3. Assim, todo corpo ordenado contém uma cópia *algébrica* de $\mathbb{Q}$.

Exercício 80. Seja K como no exercício anterior. O *corpo de frações de* K é, por definição, o corpo K' obtido de K do mesmo modo que obtivemos $\mathbb{Q}$ a partir de $\mathbb{Z}$. Por isso, $\mathbb{Q}$ também é chamado *corpo de frações de* $\mathbb{Z}$. Mostre que a imersão natural de K em K', dada por $i(n) = \frac{n}{1}$ é sobrejetora, portanto, bijetora. Ou seja, o próprio K' é uma cópia algébrica de K. Sob tal identificação, adota-se, para $a, b \in K$, com $b \neq 0$, notação análoga às estudadas nos Exercícios 74 e 75, para o produto $a \cdot b^{-1}$: a notação de divisão $a : b$ e a de fração $\frac{a}{b}$.

No que segue, os termos "limitado superiormente, inferiormente, cota superior, inferior, elemento máximo e mínimo" têm significado análogo àqueles já definidos na seção 3.3. no contexto de números inteiros.

Exercício 81. Claramente, em $\mathbb{N}$ não há elemento máximo (por quê?). No entanto, considerado como um subconjunto de $\mathbb{Q}$, poderia ocorrer dele ser um subconjunto limitado superiormente por um número racional não inteiro (*número fracionário*). Mostre que isso não pode ocorrer.

Exercício 82. Mostre que em $\mathbb{Q}$ não há elemento máximo nem mínimo.

O Exercício 81 mostra que $\mathbb{N}$ é ilimitado superiormente em $\mathbb{Q}$. Curiosamente, há corpos ordenados em que a sua cópia de naturais é limitada superiormente (veja um exemplo em [22]). Os corpos ordenados para os quais sua cópia de naturais é ilimitada superiormente chamam-se *corpos arquimedianos*.

Exercício 83. Mostre que, em um corpo ordenado $K \neq 0$, as seguintes afirmações são equivalentes:

1. K é arquimediano;

2. para todo par a, b de elementos de K, com $a \neq 0$, existe $n \in \mathbb{N}$ tal que $na > b$;

3. dado $a > 0$ em K, existe $n \in \mathbb{N}\,(\subset K)$ tal que $n^{-1} < a$.

Exercício 84. Conclua, dos exercícios anteriores, que $\mathbb{Q}$ é arquimediano e, como consequência, não é bem ordenado (conforme afirmação feita antes do Teorema 2.3.5).

Exercício 85. *(Desigualdade de Bernoulli)* Mostre, usando indução, a seguinte proposição, que é utilizada em várias demonstrações: seja K um corpo ordenado e x um elemento não nulo e maior do que -1 em K. Para todo natural n maior do que 1, tem-se $(1+x)^n > 1+nx$.

Nos exercícios seguintes, deve-se usar a identificação de $\mathbb{Z}$ com $i(\mathbb{Z})$ e, obviamente, as propriedades aritméticas de $\mathbb{Q}$.

Exercício 86. Mostre que, se $a,b,c,d \in \mathbb{Z}$, com, $b,d \neq 0$, então $\frac{a}{b} = \frac{c}{d}$ se, e somente se, existe $k \in \mathbb{Q}^*$, tal que $c = ak$ e $d = bk$.

Exercício 87. Resolva, em $\mathbb{Q}$, a inequação

$$\frac{2x-5}{7} \leq \frac{x+8}{-6}.$$

Lembremos do Ensino Fundamental que, em expressões aritméticas onde estão indicadas várias operações, convenciona-se a seguinte hierarquia na execução das operações: efetuam-se primeiro as multiplicações e divisões para depois efetuar as adições e subtrações.

Exercício 88. Interprete o significado de cada termo racional na expressão abaixo e simplifique-a:

$$\tfrac{3}{5} + (-8) : (-4) - \tfrac{2}{3} \cdot \left(-\tfrac{3}{4}\right) + (-2)^3$$

Exercício 89. Admitindo o *Teorema Fundamental da Aritmética*, mostre que:

1. a equação $x^2 = 2$ não tem solução em $\mathbb{Q}$;
2. idem para as equações $x^2 = 10$, $x^3 = 25$, $x^3 = 20$ e $x^6 = 50$;
3. generalize.

Exercício 90. Admitindo conhecidas as propriedades elementares das funções exponenciais e logarítmicas, mostre que $10^x = 15$ não tem solução em $\mathbb{Q}$, isto é, $\log_{10} 15 \notin \mathbb{Q}$. (No Exemplo 5.2.4, definiremos rigorosamente a expressão $\log_{10} 15$.)

5

Números reais

O conceito de número real é um dos mais profundos da matemática e, como vimos nas notas históricas, remonta aos gregos da escola pitagórica, com a descoberta da incomensurabilidade entre o lado e a diagonal de um quadrado. A construção desse conceito passou por Eudoxo (século IV a.C.), com sua teoria das proporções, registrada nos *Elementos* de Euclides, e só foi concretizada no século XIX, como vimos na Seção 1.1. Os matemáticos alemães, Cantor e Dedekind, construíram os números reais a partir dos racionais por métodos diferentes, respectivamente conhecidos por *Classes de Equivalência de Sequências de Cauchy* e por *Cortes de Dedekind.* O último, que apresentaremos aqui, inspirou-se na Teoria das Proporções de Eudoxo. (Para a construção via sequências de Cauchy, o leitor poderá consultar [3] e [18].)

No Ensino Fundamental, os números reais são geralmente introduzidos de uma maneira um tanto empírica e seu estudo não costuma ir além de algumas operações algébricas elementares. Basicamente, o que se diz nesse nível sobre os números reais é o seguinte: admite-se que a cada ponto de uma reta está associado um número real. Há pontos que não correspondem a números racionais (o que é fácil de veri-

ficar, usando a diagonal de um quadrado de lado 1). A esses pontos sem abscissa racional correspondem os números chamados *irracionais*. Outra forma de introduzi-los é a seguinte: admite-se ou, em alguns casos, demonstra-se que a representação decimal dos números racionais é periódica e, reciprocamente, toda representação decimal periódica corresponde à de um número racional. Conclui-se por definir número irracional como sendo aqueles (cuja existência é admitida) que possuem representação decimal não periódica. Ao conjunto constituído pelos racionais e irracionais dá-se o nome de conjunto dos números reais. Note que, em ambas as abordagens, somos conduzidos a admitir a existência de números não racionais: no primeiro caso, para dotar todo ponto da reta de uma abscissa e, no segundo, para conceber qualquer desenvolvimento decimal como número (no caso, os não periódicos). Em ambos os casos, no entanto, raramente se toca na natureza desses novos números. Uma dessas raras abordagens pode ser encontrada em [22], onde o estudo da incomensurabilidade de segmentos de reta é a via de acesso para a introdução do conceito elementar de número irracional.

Em linhas gerais, o que faremos é construir rigorosamente os números reais, tendo como ponto de partida o conjunto dos números racionais com suas propriedades algébricas e aritméticas, de modo análogo às construções anteriores (adotaremos o roteiro apresentado no clássico [28]). Definimos a noção de "corte", devida a Dedekind. Consideraremos o conjunto constituído de todos os cortes e nele definiremos duas operações, adição e multiplicação, e uma relação de ordem. Mostraremos que este conjunto possui as propriedades aritméticas de $\mathbb{Q}$ e mais uma importante propriedade que $\mathbb{Q}$ não possui: a de ser *completo*, num sentido a ser definido posteriormente.

A este conjunto de cortes chamaremos de *conjunto dos números reais*, que será denotado por $\mathbb{R}$ e, como nos casos já estudados, veremos que $\mathbb{R}$ contém uma cópia algébrica de $\mathbb{Q}$.

Vamos aos detalhes.

5.1 Cortes de Dedekind

Definição 5.1.1. Um conjunto α de números racionais diz-se um *corte* se satisfizer as seguintes condições:

i) $\emptyset \neq \alpha \neq \mathbb{Q}$;

ii) se $r \in \alpha$ e $s < r$ (s racional), então $s \in \alpha$;

iii) em α não existe elemento máximo.

Exercício 91. Mostre que:

1. o conjunto $\left\{x \in \mathbb{Q} \mid x < \frac{3}{5}\right\}$ é um corte;
2. o conjunto $\left\{x \in \mathbb{Q} \mid x > \frac{3}{5}\right\}$ não é um corte;
3. o conjunto $\left\{x \in \mathbb{Q} \mid x \leq \frac{3}{5}\right\}$ não é um corte;
4. o conjunto $\left\{x \in \mathbb{Q} \mid -3 < x < \frac{8}{5}\right\}$ não é um corte;
5. $\mathbb{Q} \setminus \{0\}$ não é um corte;
6. $\left\{1, 4, \frac{3}{5}\right\}$ não é um corte.

Proposição 5.1.1. *Sejam* α *um corte e* $r \in \mathbb{Q}$. *Então,* r *é cota superior de* α *se, e somente se,* $r \in \mathbb{Q} \setminus \alpha$.

Demonstração. Se r é cota superior de α, então r não pode pertencer a α, caso contrário r seria elemento máximo de α, contradizendo o item (iii) da definição de corte. Reciprocamente, se $r \in \mathbb{Q} \setminus \alpha$, então r é cota superior de α, pois, caso contrário, haveria $s \in \alpha$ tal que $r < s$, o que, pelo item (ii) da definição de corte, obrigaria r a pertencer a α, uma contradição. □

Proposição 5.1.2. *Se* $r \in \mathbb{Q}$ *e* $\alpha = \{x \in \mathbb{Q} \mid x < r\}$, *então* α *é um corte e* r *é a menor cota superior de* α.

Demonstração. O leitor verifica como exercício que α satisfaz as condições (i) e (ii) da Definição 5.1.1. Quanto a (iii), basta observar que se $s \in \alpha$, então $s < \frac{s+r}{2} < r$ e, como $\frac{s+r}{2} \in \mathbb{Q}$, então $\frac{s+r}{2} \in \alpha$. Assim, s não é elemento máximo de α. Esse argumento também mostra que r é a menor cota superior de α. □

Definição 5.1.2. Os cortes do tipo da proposição anterior são denominados *cortes racionais* e se representam por r^*.

Exercício 92. Mostre que todo corte que possui cota superior mínima é racional.

Mostraremos a seguir que há cortes que não possuem cota superior mínima, logo que não são racionais.

Teorema 5.1.3. *Seja* $\alpha = \{x \in \mathbb{Q}_+ \mid x^2 < 2\} \cup \mathbb{Q}_-^*$. *Então* α *é um corte que não é racional.*

Demonstração. O leitor verifica as condições (i) e (ii) da Definição 5.1.1 como exercício. Quanto à condição (iii), devemos provar que se $x \in \alpha$, então existe $y \in \alpha$ com $y > x$. Isso é óbvio se $x \leq 0$. Suponhamos então $x > 0$ com $x^2 < 2$. Para encontrar um y nas condições acima, basta encontrar $h \in \mathbb{Q}_+^*$ tal que $(x+h)^2 < 2$ e pôr $y = x+h$. Trabalhemos esta condição: temos $x^2 + 2xh + h^2 < 2$. A resolução dessa inequação em h conduziria a expressões indesejáveis no presente contexto. Não perdemos generalidade se buscarmos $h < 1$. Obtemos: $x^2 + 2xh + h^2 < x^2 + 2xh + h$ (pois $h < 1$), que fica menor do que 2 se tomarmos $h < \dfrac{2-x^2}{2x+1}$ (que faz sentido pois $x > 0$). Como a expressão $\dfrac{2-x^2}{2x+1}$ é positiva, tomando $h < \min\left\{1, \dfrac{2-x^2}{2x+1}\right\}$, $h \in \mathbb{Q}_+$ e $y = x+h$, obtemos $y^2 = (x+h)^2 < 2$, isto é, $y \in \alpha$ e $y > x$. A existência de um tal h é garantida pelo fato de $\mathbb{Q}$ ser arquimediano, conforme Exercício 84.

Mostramos, então, que α é um corte.

Verifiquemos agora que α não possui cota superior mínima. Observe primeiramente que os racionais que não pertencem a α são os positivos que têm quadrado ≥ 2. Sabemos que não existe racional cujo quadrado é 2. Logo $y \in \mathbb{Q} \setminus \alpha$ se, e somente se, $y > 0$ e $y^2 > 2$. Sabemos, da Proposição 5.1.1, que todo elemento y de $\mathbb{Q} \setminus \alpha$ é maior que qualquer elemento $x \in \alpha$. Vamos então mostrar que dado $y \in \mathbb{Q} \setminus \alpha$, existe $z \in \mathbb{Q} \setminus \alpha$ com $z < y$, de onde decorre o que queríamos provar. Novamente, busquemos h racional positivo tal que $(y-h)^2 > 2$ e façamos $z = y-h$. Não perdemos generalidade se supusermos $h < 1$.

A condição $(y-h)^2 > 2$ equivale a $y^2 - 2hy + h^2 > 2$ ou $y^2 - h(2y-h) > 2$ ou $h < \dfrac{y^2-2}{2y-h}$, já que $2y - h > 0$ (pois $y > 1$ e $h < 1$). Como $h > 0$, então $\dfrac{y^2-2}{2y-h}$ é maior do que $\dfrac{y^2-2}{2y}$. Assim, tomando $h < \min\left\{1, \dfrac{y^2-2}{2y}\right\}$ em $\mathbb{Q}_+^*$, o que é possível

pois $\mathbb{Q}$ é arquimediano, obtemos: $(y-h)^2 = y^2 - 2hy + h^2 > y^2 - 2y\frac{y^2-2}{2y} + h^2 = 2 + h^2 > 2$. □

Notação. Denotaremos por $\mathcal{C}$ o conjunto de todos os cortes.

5.2 Relação de ordem e operações com cortes

Definiremos em $\mathcal{C}$ duas operações, "+" e ".", e uma relação de ordem. Começaremos pela relação de ordem, pois ela será indispensável na definição da multiplicação.

Definição 5.2.1. Sejam $\alpha, \beta \in \mathcal{C}$. Dizemos que α *é menor do que* β e escrevemos $\alpha < \beta$ quando $\beta \setminus \alpha \neq \emptyset$.

Valem aqui as observações notacionais para desigualdades análogas às feitas após as Definições 3.3.1 e 4.3.1.

Exemplo 5.2.1.

1) $4^* > \left(\frac{3}{5}\right)^*$, pois $2 \in 4^* \setminus \left(\frac{3}{5}\right)^*$;

2) $1^* > 0^*$, pois $\frac{1}{2} \in 1^* \setminus 0^*$;

3) $(-3)^* < 0^*$, pois $-1 \in 0^* \setminus (-3)^*$;

4) Se α é o corte do Teorema 5.1.3, então $\alpha < 2^*$, pois $\frac{18}{10} \in 2^* \setminus \alpha$.

Definição 5.2.2. Se $\alpha \in \mathcal{C}$ e $\alpha > 0^*$, α chama-se *corte positivo*. Se $\alpha < 0^*$, α é dito *corte negativo*. Se $\alpha \geq 0^*$, α chama-se corte *não negativo* e se $\alpha \leq 0^*$, α chama-se *não positivo*.

Exercício 93. Mostre que, para $\alpha, \beta \in C$, valem as equivalências:

1. $\alpha < \beta \Leftrightarrow \alpha \subset \beta$ e $\alpha \neq \beta$;

2. $\alpha \leq \beta \Leftrightarrow \alpha \subset \beta$.

Teorema 5.2.1. *(Tricotomia) Para $\alpha, \beta \in C$, temos que uma e apenas uma das possibilidades a seguir ocorre.*

$$\alpha = \beta \qquad ou \qquad \alpha < \beta \qquad ou \qquad \alpha > \beta.$$

Demonstração. É claro que $\alpha = \beta$ exclui as outras duas possibilidades, pela definição de igualdade de conjuntos. De modo análogo, as possibilidades $\alpha < \beta$ ou $\alpha > \beta$ claramente excluem $\alpha = \beta$, pelo exercício precedente. Mostremos que as desigualdades também se excluem mutuamente. Suponhamos o contrário, isto é, que $\alpha < \beta$ e $\alpha > \beta$ ocorram simultaneamente. Então, existem $r \in \beta \setminus \alpha$ e $s \in \alpha \setminus \beta$. De $r \in \beta$ e $s \notin \beta$ resulta $r < s$, e de $s \in \alpha$ e $r \notin \alpha$ resulta $s < r$, contradizendo a lei da tricotomia em $\mathbb{Q}$. Concluímos que no máximo uma das três possibilidades ocorre. Para mostrar que uma delas necessariamente ocorre, temos que $\alpha = \beta$ ou $\alpha \neq \beta$. Se $\alpha = \beta$, nada há a provar. Suponhamos $\alpha \neq \beta$. Então $\alpha \setminus \beta \neq \emptyset$ ou $\beta \setminus \alpha \neq \emptyset$ (pois, caso contrário, $\alpha = \beta$). No primeiro caso, $\beta < \alpha$ e, no segundo caso, $\alpha < \beta$. □

Teorema 5.2.2. *A relação $\leq$ é uma relação de ordem em C.*

Demonstração. A prova da reflexividade e da antissimetria de $\leq$ ficam a cargo do leitor. Quanto à transitividade, ela segue do Exercício 93 e do fato da inclusão de conjuntos ser transitiva. □

Vamos agora à definição das operações de *adição* e de *multiplicação* em $\mathcal{C}$. Comecemos com o teorema a seguir.

Teorema 5.2.3. *Sejam* $\alpha, \beta \in \mathcal{C}$. *Se* $\gamma = \{r+s \mid r \in \alpha \text{ e } s \in \beta\}$, *então* $\gamma \in \mathcal{C}$.

Demonstração. Mostremos que γ satisfaz as três condições da Definição 5.1.1.

(i) É claro que $\gamma \neq \emptyset$. Sejam $t \in \mathbb{Q} \setminus \alpha$ e $u \in \mathbb{Q} \setminus \beta$. Como $t > r$, $\forall r \in \alpha$ e $u > s$, $\forall s \in \beta$, então $t + u > r + s$, $\forall r \in \alpha$, $\forall s \in \beta$, isto é, $t + u \notin \gamma$, logo $\gamma \neq \mathbb{Q}$.

(ii) Sejam $r \in \gamma$ e $s < r$ (s racional). Mostremos que $s \in \gamma$; r é do tipo $p + q$, com $p \in \alpha$ e $q \in \beta$. Então, de $s < p + q$, podemos escrever $s = p + q'$ com $q' < q$ e, portanto, $q' \in \beta$. Logo, $s = p + q'$, com $p \in \alpha$ e $q' \in \beta$, isto é, $s \in \gamma$.

(iii) Vamos mostrar que em γ não há elemento máximo, isto é, se $r \in \gamma$, existe $s \in \gamma$ com $s > r$. Temos: $r = p + q$, com $p \in \alpha$ e $q \in \beta$. Como existe $p' \in \alpha$ com $p' > p$, o racional $s = p' + q \in \gamma$ e é maior do que r. □

Definição 5.2.3. Para $\alpha, \beta \in \mathcal{C}$, definimos $\alpha + \beta$ como sendo o corte do teorema anterior, ou seja,

$$\alpha + \beta = \{r + s \mid r \in \alpha \text{ e } s \in \beta\}.$$

Exercício 94. Mostre que se $p, q \in \mathbb{Q}$, então $p^* + q^* = (p+q)^*$. Prove também que $p^* \leq q^*$ se, e somente se, $p \leq q$.

Teorema 5.2.4. *A adição em* $\mathcal{C}$ *é comutativa, associativa e tem* 0^* *como elemento neutro.*

Demonstração. A comutatividade e a associatividade são herdadas das propriedades análogas da adição em $\mathbb{Q}$. O leitor deve provar esses fatos como exercício. Para mostrar que $\alpha + 0^* = \alpha$, $\forall\, \alpha \in \mathcal{C}$, vamos verificar as duas inclusões: $\alpha + 0^* \subset \alpha$ e

$\alpha \subset \alpha + 0^*$. Seja $r \in \alpha + 0^*$. Então $r = p + q$, com $p \in \alpha$ e $q \in 0^*$, isto é, $q < 0$. Assim, $r < p \in \alpha$ e, portanto, $r \in \alpha$. Logo, $\alpha + 0^* \subset \alpha$. Seja agora $r \in \alpha$. Tomando $s \in \alpha$ com $s > r$, podemos expressar r como $r = s + (r - s)$, onde $r - s < 0$ e, portanto, ele pertence 0^*. Assim, $r \in \alpha + 0^*$ e $\alpha \subset \alpha + 0^*$. □

Exercício 95. Mostre que se $s \in \mathbb{Q}$ e $r \in \mathbb{Q}^*_+$, então $\{s + mr \mid m \in \mathbb{N}\}$ não é limitado superiormente em $\mathbb{Q}$ (relembre o Exercício 81).

Para mostrar que todo corte tem simétrico (inverso aditivo), comecemos com um lema.

Lema 5.2.5. *Sejam $\alpha \in C$ e $r \in \mathbb{Q}^*_+$. Então existem números racionais p e q tais que $p \in \alpha$, $q \notin \alpha$, q não é cota superior mínima de α e $q - p = r$.*

Demonstração. Tomemos s arbitrário em α e consideremos a sequência

$$s,\ s + r,\ s + 2r,\ s + 3r,\ \ldots,\ s + nr,\ \ldots\ .$$

Como essa sequência não é limitada superiormente (Exercício 95), α é limitado superiormente e $s \in \alpha$, então existe um único inteiro $m \geq 0$ tal que $s + mr \in \alpha$ e $s + (m+1)r \notin \alpha$ (prove esta afirmação através do Princípio da Boa Ordem). Se $s + (m+1)r$ não for cota superior mínima de α, tome $p = s + mr$ e $q = s + (m+1)r$. Se $s + (m+1)r$ for a cota superior mínima de α, tome $p = s + mr + \frac{r}{2}$ e $q = s + (m+1)r + \frac{r}{2}$. □

Teorema 5.2.6. *Seja $\alpha \in C$. Existe um único $\beta \in C$ tal que $\alpha + \beta = 0^*$. Como nos casos dos inteiros e racionais, tal β denota-se por $-\alpha$ e se chama simétrico (ou inverso aditivo) de α.*

Demonstração. A demonstração da unicidade do simétrico em qualquer estrutura algébrica que possua uma adição associativa e com elemento neutro é sempre a mesma, conforme o Exercício 39. A título de exercício, vamos refazê-la neste caso particular: suponhamos $\alpha + \beta_1 = \alpha + \beta_2 = 0^*$. (Lembre-se de que a adição de cortes é comutativa.) Obtemos:

$$\beta_2 = \beta_2 + 0^* = \beta_2 + (\alpha + \beta_1) = (\beta_2 + \alpha) + \beta_1 = 0^* + \beta_1 = \beta_1.$$

A demonstração da existência do simétrico depende, no entanto, da situação considerada. Para se ter uma ideia de como construir o simétrico de α, consideremos inicialmente um caso particular simples, digamos, $\alpha = 3^*$. É de se esperar que seu simétrico, $-(3^*)$, seja $(-3)^*$. Temos:

$$3^* = \{r \in \mathbb{Q} \mid r < 3\} \ , \ (-3)^* = \{s \in \mathbb{Q} \mid s < -3\}$$

e $3^* + (-3)^* = \{r + s \in \mathbb{Q} \ \mid \ s \in 3^* \text{ e } s \in (-3)^*\}$. Para verificar se $3^* + (-3)^*$ é 0^*, verifiquemos as duas inclusões pertinentes: $3^* + (-3)^* \subset 0^*$ e vice-versa.

Seja $t \in 3^* + (-3)^*$. Então $t = r + s$, onde $r < 3$ e $s < -3$. Logo, $t = r + s < 3 + (-3) = 0$, portanto $t \in 0^*$.

Seja agora $t \in 0^*$, ou seja, $t < 0$. Para fixar as ideias, tomemos $t = -2$. Como expressar o -2 como uma soma $r + s$ com $r < 3$ e $s < -3$? Pelo Lema 5.2.5, existem $r \in 3^*$ e $r' \notin 3^*$ com $r' \neq 3$ (= cota superior mínima de 3^*), tais que $r' - r = 2$, ou ainda, $-2 = r + (-r')$. Como $r' > 3$, então $-r' < -3$, ou seja, $-r' \in (-3)^*$.

Tentemos utilizar as ideias desse caso particular no caso geral. Dado $\alpha \in \mathcal{C}$, o candidato a $-\alpha$ é o conjunto obtido pelos negativos dos elementos que estão fora de α, com exceção da eventual cota superior mínima de α. Mais precisamente, seja $\beta = \{p \in \mathbb{Q} \mid -p \notin \alpha \text{ e } -p \text{ não é cota superior mínima de } \alpha\}$. (Observe que $(-3)^* = \{p \in \mathbb{Q} \mid -p \notin 3^* \text{ e } -p \text{ não é cota superior mínima de } 3^*\}$. No caso geral,

não temos necessariamente cortes racionais e, então, o símbolo $(-\alpha)^*$ pode não fazer sentido.)

Mostremos que β é um corte e que $\alpha+\beta = 0^*$. Verifiquemos as três condições da definição de corte: (i) e (ii) ficam a cargo do leitor. Quanto a (iii), seja $r \in \beta$. Queremos encontrar $s > r$ em β. Como $-r$ é cota superior de α mas não é mínima, então existe $t \in \mathbb{Q}$, $-t < -r$, tal que $-t$ é cota superior de α e, portanto, $-t \notin \alpha$. Seja $s = \dfrac{r+t}{2}$. Temos: $-t < -s < -r$, de modo que $-s$ é cota superior de α mas não é mínima, logo $s \in \beta$ e $s > r$, como queríamos.

Vamos verificar agora que $\alpha+\beta = 0^*$. Seja $t \in \alpha+\beta$. Então $t = r+s$, com $r \in \alpha$ e $s \in \beta$. Como $-s \notin \alpha$, então $-s > r$, de modo que $0 > r+s = t$, ou seja, $t \in 0^*$. Reciprocamente, suponhamos $t \in 0^*$, isto é, $t < 0$. Sejam $r \in \alpha$ e $r' \notin \alpha$ (r' não sendo cota superior mínima de α), tais que $r' - r = -t$ (Lema 5.2.5). Segue que $t = r + (-r')$, com $r \in \alpha$ e $-r' \in \beta$, ou seja, $t \in \alpha+\beta$. □

Definição 5.2.4. Como nos casos de $\mathbb{Z}$ e $\mathbb{Q}$, definimos a *subtração* em C por $\alpha - \beta = \alpha + (-\beta)$, $\forall \alpha, \beta \in C$.

Exercício 96. Encontre o simétrico do corte α do Teorema 5.1.3.

Proposição 5.2.7. *Para $\alpha, \beta, \gamma \in C$, vale:*

i) $-(-\alpha) = \alpha$;

ii) $-\alpha + \beta = \beta - \alpha$;

iii) $\alpha - (-\beta) = \alpha + \beta$;

iv) $-\alpha - \beta = -(\alpha + \beta)$;

v) $\alpha - (\beta + \gamma) = \alpha - \beta - \gamma$;

Demonstração. Como nas proposições análogas para os casos de $\mathbb{Z}$ e de $\mathbb{Q}$, a demonstração é estritamente algébrica, isto é, apenas utiliza as propriedades da adição e de elemento simétrico, que são as mesmas nas duas situações e na presente. Confirme este fato realizando você a demonstração desta proposição. □

Teorema 5.2.8. *(Compatibilidade da relação de ordem com a adição) Sejam* $\alpha, \beta, \gamma \in C$ *tais que* $\alpha \leq \beta$. *Então* $\alpha + \gamma \leq \beta + \gamma$.

Demonstração. $\alpha \leq \beta \Leftrightarrow \alpha \subset \beta$. (Veja o Exercício 93.) Seja $t \in \alpha + \gamma$, isto é, $t = r + s$ com $r \in \alpha$ e $s \in \gamma$. Como $\alpha \subset \beta$, então $r \in \beta$ e $t = r + s \in \beta + \gamma$, ou seja, $\alpha + \gamma \subset \beta + \gamma$. Portanto $\alpha + \gamma \leq \beta + \gamma$. □

Exercício 97. Seja $\alpha \in C$. Mostre que se $\alpha \geq 0$, então $-\alpha \leq 0$.

Definiremos agora uma multiplicação em C, seguindo os mesmos passos realizados na definição da adição e de suas propriedades. Embora o tratamento da multiplicação em C seja tecnicamente um pouco mais complicado, ele segue bem de perto o tratamento e as demonstrações para o caso da adição. Por essa razão, omitiremos a maioria delas, deixando-as como exercício para o leitor interessado.

Pela nossa definição de adição, o Exercício 94 mostra que, por exemplo, $3^* + 5^* = 8^*$. Gostaríamos de definir multiplicação de modo que $3^* \cdot 5^* = 15^*$.

Uma primeira tentativa seria transferir a definição de adição para o caso da multiplicação do seguinte modo: $3^* \cdot 5^* = \{p \cdot q \mid p \in 3^* \text{ e } q \in 5^*\}$. No entanto, não obteríamos 15^* como resultado pois o racional $(-10) \cdot (-5) = 50$ é elemento do conjunto acima e não é elemento de 15^*. Aliás, o conjunto acima sequer é um corte! (Por quê?)

Vemos, então, que a transferência direta do caso aditivo não funciona bem. No entanto, alguns ajustes conduzem à definição satisfatória.

Teorema 5.2.9. *Para $\alpha, \beta \in C$ com $\alpha \geq 0^*$ e $\beta \geq 0^*$, seja*

$$\gamma = \mathbb{Q}^*_- \cup \{r \in \mathbb{Q} \mid r = pq, \text{ com } p \in \alpha, \, q \in \beta, \, p \geq 0 \text{ e } q \geq 0\}.$$

Então, γ é um corte e $\gamma \geq 0$.

Exercício 98. Demonstre o Teorema 5.2.9.

Definição 5.2.5. Se $\alpha, \beta \in C$ e $\alpha \geq 0^*$, $\beta \geq 0^*$, definimos o produto $\alpha \cdot \beta$ (ou $\alpha\beta$) como sendo o corte γ do teorema anterior.

Para definir produto de cortes que contêm fatores negativos, começamos com a noção de *valor absoluto* de um corte, similar à Definição 3.3.4 de módulo de um número inteiro.

Definição 5.2.6. Dado $\alpha \in C$, definimos o *valor absoluto de* α (ou o *módulo de* α), representado por $|\alpha|$, do seguinte modo:

$$|\alpha| = \begin{cases} \alpha, & \text{se } \alpha \geq 0^*; \\ -\alpha, & \text{se } \alpha < 0^*. \end{cases}$$

Exercício 99. Mostre que, para qualquer $\alpha \in \mathcal{C}$, tem-se:

1) $|\alpha| \geq 0^*$;

2) $|\alpha| = 0^*$ se, e somente se, $\alpha = 0^*$;

3) $|\alpha| = |-\alpha|$.

Definição 5.2.7. Se $\alpha, \beta \in \mathcal{C}$, definimos:

$$\alpha\beta = \begin{cases} -(|\alpha||\beta|), & \text{se} \quad \alpha \leq 0^*, \beta \geq 0^*; \\ -(|\alpha||\beta|), & \text{se} \quad \alpha \geq 0^*, \beta \leq 0^*; \\ |\alpha||\beta|, & \text{se} \quad \alpha < 0^*, \beta < 0^*. \end{cases}$$

Proposição 5.2.10. *Para* $\alpha, \beta \in \mathcal{C}$, *temos* $(-\alpha)\beta = \alpha(-\beta) = -\alpha\beta$ *e* $(-\alpha)(-\beta) = \alpha\beta$.

Demonstração. A demonstração das duas primeiras igualdades é subdividida em casos, todos tratados de maneira similar. A terceira igualdade é consequência das duas anteriores, usando regras de sinais dadas na Proposição 5.2.7. Demonstraremos apenas a igualdade $(-\alpha)\beta = -\alpha\beta$ para o caso $\alpha \geq 0$ e $\beta \geq 0$ e deixaremos as demais como exercício para o leitor. Nesse caso, por definição de multiplicação, já que $-\alpha \leq 0$, temos:
$(-\alpha)\beta = -(|-\alpha|\,|\beta|) = -([-(-\alpha)]\beta) = -(\alpha\beta)$. Analogamente, verificamos que $\alpha(-\beta) = -(\alpha\beta)$. □

Teorema 5.2.11. *A multiplicação de cortes é comutativa, associativa, tem 1^* como elemento neutro e, se $\alpha, \beta, \gamma \in C$, vale:*

i) $\alpha(\beta+\gamma) = \alpha\beta + \alpha\gamma$ *(distributividade);*

ii) $\alpha.0^* = 0^*$*;*

iii) se $\alpha \leq \beta$ *e* $\gamma \geq 0^*$*, então* $\alpha\gamma \leq \beta\gamma$*;*

iv) se $\alpha \leq \beta$ *e* $\gamma < 0^*$*, então* $\alpha\gamma \geq \beta\gamma$*;*

v) se $\alpha \neq 0^*$ *em C, existe um único* $\beta \in C$ *tal que* $\alpha\beta = 1^*$*. Esse corte chama-se inverso de* α *e é denotado por* α^{-1}*.*

Demonstração. Conforme já comentado, as demonstrações das propriedades da multiplicação de cortes são similares porém mais complicadas do que as da adição. Para ilustrar, demonstraremos (i) e deixaremos os demais itens como exercícios para o leitor interessado. A estrutura da demonstração é a seguinte: a distributividade será inicialmente demonstrada para α, β e γ maiores ou iguais a 0. Os demais casos são consequências desse e das propriedades já estudadas, principalmente as regras de sinais. Assim, suponhamos $\alpha, \beta, \gamma \geq 0$. Caracterizaremos os elementos dos conjuntos de racionais $A = \alpha(\beta+\gamma)$ e $B = \alpha\beta + \alpha\gamma$ e mostraremos que $A = B$. Temos:

$$\beta+\gamma = \{y+z \in \mathbb{Q} \mid y \in \beta \text{ e } z \in \gamma\}$$

e

$$A = \alpha(\beta+\gamma) = \mathbb{Q}_-^* \cup \{r \in \mathbb{Q} \mid r = pq, \text{ com } 0 \leq p \in \alpha \text{ e } 0 \leq q \in \beta+\gamma\}.$$

Como $0 \leq q \in \beta + \gamma$, então $0 \leq q = y + z$, com $y \in \beta$ e $z \in \gamma$. Logo, os elementos de A ou são racionais negativos, ou são da forma:

$r = py + pz$, com $0 \leq p \in \alpha$, $y \in \beta$, $z \in \gamma$ e $0 \leq y + z$.

Por outro lado, temos:

$$\alpha\beta = \mathbb{Q}_-^* \cup \{r' \in \mathbb{Q} \mid r' = p'y',\ com\ 0 \leq p' \in \alpha\ e\ 0 \leq y' \in \beta\},$$

$$\alpha\gamma = \mathbb{Q}_-^* \cup \{r'' \in \mathbb{Q} \mid r'' = p''z'',\ com\ 0 \leq p'' \in \alpha\ e\ 0 \leq z'' \in \gamma\}\ e$$

$$B = \alpha\beta + \alpha\gamma = \{s + t \in \mathbb{Q} \mid s \in \alpha\beta\ e\ t \in \alpha\gamma\}.$$

Assim, os elementos de B são de uma das formas seguintes:

a) $a + b$, com $a, b \in \mathbb{Q}_-^*$;

b) $a + p''z''$, com $a \in \mathbb{Q}_-^*$, $0 \leq p'' \in \alpha$ e $0 \leq z'' \in \gamma$;

c) $p'y' + b$, com $b \in \mathbb{Q}_-^*$, $0 \leq p' \in \alpha$ e $0 \leq y' \in \beta$;

d) $p'y' + p''z''$, com $0 \leq p' \in \alpha$, $0 \leq y' \in \beta$, $0 \leq p'' \in \alpha$ e $0 \leq z'' \in \gamma$.

Devemos provar que qualquer elemento de A é de uma das formas presentes em B e vice-versa. Vamos verificar que a segunda forma presente em A é elemento de B e os elementos de B da forma (d) estão em A. As demais verificações ficam para o leitor. Assim, consideremos um elemento de A da forma $py + pz$, com $0 \leq p \in \alpha$, $y \in \beta$, $z \in \gamma$ e $0 \leq y + z$. Novamente, há subcasos a considerar: se y e z são maiores ou iguais a 0, é claro que $py + pz \in B$. Se $y < 0$ e $z \geq 0$, então $py + pz = a + pz$, com $a \leq 0$, que é da forma (b) ou (d) de B. Os demais subcasos também são deixados para reflexão do leitor. Concluímos que $A \subset B$.

Tomemos agora um elemento de B da forma (d): $p'y' + p''z''$, com $0 \leq p' \in \alpha$,

$0 \le y' \in \beta$, $0 \le p'' \in \alpha$ e $0 \le z'' \in \gamma$. Suponhamos $p \ge p'$. Temos:

$p'y' + p''z'' = p'y' + p'z'' - p'z'' + p''z'' = p'(y' - z'') - z''(p' - p'')$. O primeiro somando da última expressão é elemento de A e o segundo é um racional não positivo. Como A é um corte, essa expressão é um elemento de A. Assim, $B \subset A$.

Dessa forma, concluímos a demonstração da distributividade para o caso em que α, β e γ são maiores ou iguais a 0. Conforme comentado no início desta demonstração, os demais casos são consequências desse e das demais propriedades aritméticas já estudadas.

Analisemos o caso em que em que $\alpha < 0$ e $\beta, \gamma \ge 0$. Temos:

$\alpha(\beta+\gamma) = -(|\alpha||\beta+\gamma|) = -[(-\alpha)(\beta+\gamma)] = -[(-\alpha)\beta + (-\alpha)\gamma] = -[-\alpha\beta - \alpha\gamma] = \alpha\beta + \alpha\gamma$. Para as duas últimas igualdades, usamos a proposição anterior. Os demais casos são tratados de forma similar, usando-se as informações adicionais seguintes, ficando os detalhes, mais uma vez, como um instrutivo exercício para o leitor:

1. Se β e γ são menores ou iguais a 0, então $\beta + \gamma = -(|\beta| + |\gamma|)$;
2. Se $\beta \ge \gamma \ge 0$ e $\alpha \ge 0$, então, temos: $\alpha\beta = \alpha(\beta - \gamma + \gamma) = \alpha(\beta - \gamma) + \alpha\gamma$, de onde segue que $\alpha(\beta - \gamma) = \alpha\beta - \alpha\gamma$.

□

Exercício 100. Mostre, usando (v) do teorema anterior, que $\alpha\beta = 0^*$ se, e somente se, $\alpha = 0^*$ ou $\beta = 0^*$.

Exercício 101. Se $p, q \in \mathbb{Q}$, mostre que $p^* \cdot q^* = (pq)^*$.

Proposição 5.2.12. *Se $\alpha \in C$, temos que $r \in \alpha$ se, e somente se, $r^* < \alpha$.*

Demonstração. Se $r \in \alpha$, como $r \notin r^*$, então $r^* < \alpha$. Reciprocamente, se $r^* < \alpha$, existe $s \in \alpha \setminus r^*$. Temos então que $s \ge r$ e $s \in \alpha$. Logo, $r \in \alpha$. □

Teorema 5.2.13. *Se $\alpha, \beta \in C$ e $\alpha < \beta$, então existe um corte racional r^* tal que $\alpha < r^* < \beta$.*

Demonstração. *1º caso*: α é um corte racional, digamos, $\alpha = s^*$. Como $\alpha < \beta$, existe $r \in \beta \setminus \alpha$ (r racional), com $r > s$. (Caso contrário, $\beta \setminus \alpha = \{s\}$, isto é, $\beta = \alpha \cup \{s\}$, contrariando a condição (iii) da definição de corte.) De $r \in \beta$ e $r \notin r^*$, obtemos $r^* < \beta$. Como $s < r$, então $\alpha = s^* < r^*$.

2º caso: α não é um corte racional. Como $\alpha < \beta$, existe $r \in \beta \setminus \alpha$ (r racional). De $r \in \beta \setminus r^*$, obtemos $r^* < \beta$. Como r é cota superior de α e α não é corte racional, então r não é cota superior mínima de α e, daí, existe $s \in r^* \setminus \alpha$, ou seja, $\alpha < r^*$. □

Temos, então, C munido de duas operações e uma relação de ordem obedecendo às mesmas leis aritméticas dos racionais. Assim, resgatando a linguagem algébrica introduzida na Seção 4.4., C é, como $\mathbb{Q}$, um *corpo ordenado*. Em particular, define-se também a divisão em C e adota-se a notação de fração $\frac{\alpha}{\beta}$, conforme Exercícios 74 e 75. Além disso, a aplicação $j : \mathbb{Q} \to C$ dada por $j(r) = r^*$ é injetora e preserva adição, multiplicação e ordem, conforme os Exercícios 94 e 101.

Mais uma vez, obtivemos uma cópia algébrica de um conjunto em outro, desta vez, $j(\mathbb{Q})$ é uma cópia de $\mathbb{Q}$ em C, sendo $j(\mathbb{Q})$ precisamente o conjunto dos cortes racionais. O Teorema 5.1.3 mostra que há em C cortes não racionais. Assim, $C \setminus j(\mathbb{Q}) \neq \emptyset$.

Definição 5.2.8. O conjunto $\mathcal{C}$ dos cortes será, a partir de agora, denominado de *conjunto dos números reais* e denotado por $\mathbb{R}$. Os cortes racionais serão identificados, via a injeção j, com os *números racionais*. Todo corte que não for racional será denominado *número irracional.*

Notação: a identificação de $j(\mathbb{Q})$ com $\mathbb{Q}$ nos permite escrever $\mathbb{Q} \subset \mathbb{R}$. O conjunto $\mathbb{R} \setminus \mathbb{Q}$ representa o *conjunto dos números irracionais.*

Exercício 102. Levando em consideração as observações acima, esclareça em que contexto cada uma das afirmações seguintes pode ser considerada verdadeira ou falsa:

1. um número real é um conjunto de números racionais;
2. todo número racional é real.

Os resultados seguintes mostram que, apesar da semelhança entre as propriedades aritméticas e de ordem entre $\mathbb{Q}$ e $\mathbb{R}$, há uma importante propriedade de $\mathbb{R}$ que $\mathbb{Q}$ não possui, a da *completude*.

Teorema 5.2.14. *(Dedekind) Sejam A e B subconjuntos de $\mathbb{R}$ tais que:*

i) $\mathbb{R} = A \cup B$;

ii) $A \cap B = \emptyset$;

iii) $A \neq \emptyset$ *e* $B \neq \emptyset$;

iv) se $\alpha \in A$ *e* $\beta \in B$, *então* $\alpha < \beta$.

Nessas condições existe um, e apenas um, número real γ tal que $\alpha \leq \gamma \leq \beta$, para todo $\alpha \in A$ e para todo $\beta \in B$.

Demonstração. Unicidade: suponhamos que existam dois números γ_1 e γ_2, com $\gamma_1 < \gamma_2$ nas condições do enunciado. Consideremos γ_3 tal que $\gamma_1 < \gamma_3 < \gamma_2$, o que é

possível pelo Teorema 5.2.13 (ou por um argumento análogo ao realizado no item 6 do Exercício 76). De $\gamma_3 < \gamma_2$ resulta $\gamma_3 \in A$, pois $\beta \geq \gamma_2 (> \gamma_3)$, para todo $\beta \in B$ e $A \cup B = \mathbb{R}$. Analogamente, de $\gamma_1 < \gamma_3$, resulta $\gamma_3 \in B$. Obtemos então $\gamma_3 \in A \cap B$, uma contradição.

Existência: seja $\gamma = \{r \in \mathbb{Q} \mid r \in \alpha, \text{ para algum } \alpha \in A\}$. Mostremos que γ é um corte nas condições requeridas.

i) $\emptyset \neq \gamma \neq \mathbb{Q}$: a desigualdade $\emptyset \neq \gamma$ resulta imediatamente de $A \neq \emptyset$. Para mostrar que $\gamma \neq \mathbb{Q}$, tomemos $\beta \in B$. Seja $s \notin \beta$ um racional. Como $\alpha \subset \beta$, $\forall \alpha \in A$, então $s \notin \alpha$, $\forall \alpha \in A$, de onde resulta $s \notin \gamma$.

ii) Se $r \in \gamma$ e $s < r$, então $s \in \gamma$: temos que $r \in \alpha$ para algum $\alpha \in A$ e, como $s < r$, então $s \in \alpha$ de onde segue que $s \in \gamma$.

iii) Se $r \in \gamma$, então existe $s > r$ com $s \in \gamma$: temos que $r \in \alpha$ para algum $\alpha \in A$ e, como α é um corte, existe $s > r$ em α, logo $s \in \gamma$.

Assim, γ é um número real e temos que $\alpha \leq \gamma$, $\forall \alpha \in A$, pois, pela definição de γ, sabemos que $\alpha \subset \gamma$, $\forall \alpha \in A$.

Mostremos agora que $\gamma \leq \beta$, $\forall \beta \in B$. Suponhamos que exista $\beta \in B$ com $\beta < \gamma$. Neste caso, existe um racional $r \in \gamma \setminus \beta$. Por pertencer a γ, r é um elemento de algum $\alpha \in A$ e, não sendo elemento de β, obtemos $\beta < \alpha$, contrariando a hipótese (iv). □

Neste teorema está a essência da grande diferença entre $\mathbb{Q}$ e $\mathbb{R}$, conforme o leitor deve verificar no exercício seguinte.

Exercício 103. Considere os seguintes subconjuntos de $\mathbb{Q}$:

$$A = \{x \in \mathbb{Q}_+ \mid x^2 < 2\} \cup \mathbb{Q}_-^* \text{ e } B = \{x \in \mathbb{Q}_+ \mid x^2 > 2\}.$$

Mostre que A e B satisfazem as hipóteses do teorema anterior, com $\mathbb{Q}$ em lugar de $\mathbb{R}$, mas que não existe $r \in \mathbb{Q}$ satisfazendo $s \leq r$, $\forall s \in A$ e $r \leq t$, $\forall t \in B$.

Note que o teorema e o exercício anteriores nos dizem, informalmente, que em $\mathbb{R}$ não há "lacunas", mas em $\mathbb{Q}$, há. Por esta razão, dizemos que $\mathbb{R}$ possui a *propriedade da completude* ou que $\mathbb{R}$ é *completo*.

Corolário 5.2.15. *Nas condições do teorema anterior, ou existe em A um número máximo, ou, em B, um número mínimo.*

Demonstração. Seja γ como no teorema anterior. Então γ está em A ou em B, pela hipótese (i) e, por (ii), em apenas um desses conjuntos.

Se $\gamma \in A$, então γ é elemento máximo de A e, se $\gamma \in B$, γ é elemento mínimo de B. □

Observe ainda que se o conjunto A do Teorema 5.2.14 não contiver γ, então ele é um *corte em* $\mathbb{R}$, no sentido da Definição 5.1.1 de corte em $\mathbb{Q}$. A diferença entre ambas as situações é que em $\mathbb{Q}$ não se tem necessariamente, como no Teorema 5.2.14 para os números reais, um elemento como γ. Essas lacunas é que geram os cortes (números) irracionais. Como tais lacunas não ocorrem em $\mathbb{R}$, então cortes em $\mathbb{R}$ não geram elementos novos.

Adotaremos a usual notação para *intervalos* de números reais, que são os subconjuntos de $\mathbb{R}$ dos seguintes tipos, onde a e b são reais com $a < b$:

1. $]a,b[= \{x \in \mathbb{R} \mid a < x < b\}$;
2. $[a,b[= \{x \in \mathbb{R} \mid a \leq x < b\}$;

3. $]a,b] = \{x \in \mathbb{R} \mid a < x \leq b\}$;

4. $[a,b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$;

5. $]a,+\infty[= \{x \in \mathbb{R} \mid x > a\}$ e, analogamente, para os intervalos:

$[a,+\infty[$; $]-\infty,a[$; $]-\infty,a]$ e $]-\infty,+\infty[= \mathbb{R}$.

A interpretação geométrica que adotamos intuitivamente para o conjunto dos números reais desde o Ensino Fundamental, através de uma "reta", é tornada rigorosa com o estudo axiomático da geometria euclidiana plana, que não faremos aqui, o que não nos impedirá de continuar usando nossa intuição.

O próximo teorema é de importância fundamental na análise matemática. Dele decorrem os famosos Teorema do Valor Intermediário e o Teorema de Weierstrass. O primeiro diz que toda função f contínua, definida num intervalo fechado $[a,b]$, a valores reais, assume todos os valores entre $f(a)$ e $f(b)$. O segundo diz que uma tal função assume um valor máximo e um valor mínimo nesse intervalo. Desses dois teoremas, decorrem todos os demais teoremas do Cálculo Diferencial e Integral de funções reais a valores reais, incluindo o Teorema Fundamental do Cálculo.

Comecemos com algumas definições:

Definição 5.2.9.

i) Seja A um subconjunto de $\mathbb{R}$. Dizemos que A é *limitado superiormente* se existe $k \in \mathbb{R}$ tal que $k \geq x$, $\forall x \in A$. Um tal k diz-se *cota superior de* A (como já definido para subconjuntos de $\mathbb{Z}$, conforme a Definição 3.3.3).

ii) De modo análogo, define-se subconjunto de $\mathbb{R}$ *limitado inferiormente* e *cota inferior*.

iii) A diz-se *limitado* se for limitado superiormente e limitado inferiormente.

iv) Suponhamos que A seja limitado superiormente e que exista uma cota superior de A, digamos s, que seja mínima (no sentido de que qualquer cota superior de A seja maior ou igual a s). Neste caso s diz-se *supremo de A* e é denotado por $\sup A$.

v) De modo análogo, define-se *ínfimo de A* (para conjuntos A limitados inferiormente), denotado por $\inf A$, como sendo uma cota inferior máxima para o conjunto A.

Exemplo 5.2.2.

1. Seja $A = \left\{1, \frac{1}{2}, \frac{1}{3}, \ldots, \frac{1}{n}, \ldots\right\} = \left\{\frac{1}{n} \mid n \in \mathbb{N}^*\right\}$. Temos: A é limitado, $\sup A = 1$ e $\inf A = 0$. Observe que $\sup A \in A$, mas $\inf A \notin A$.

2. $A = \{x \in \mathbb{R} \mid x \geq 0\}$. A é limitado inferiormente, mas não é limitado superiormente. Seu ínfimo é 0.

Exercício 104. Mostre que um subconjunto não vazio de $\mathbb{R}$ admite, no máximo, um supremo.

Teorema 5.2.16. *Se $X \subset \mathbb{R}$ é um conjunto não vazio e limitado superiormente, então existe* $\sup X$.

Demonstração. Definamos $A = \{\alpha \in \mathbb{R} \mid \alpha < x$, para algum $x \in X\}$, isto é, A é o conjunto constituído precisamente pelos números reais que não são cotas superiores de X.

Seja $B = \mathbb{R} \setminus A$, isto é, B é o conjunto constituído pelas cotas superiores de X. Vamos verificar que A e B satisfazem as condições do Teorema 5.2.14.

As condições (i) e (ii) são claramente válidas. Quanto a (iii), temos que, sendo $X \neq \emptyset$, existe $x \in X$ e, portanto, qualquer $\alpha < x$ é elemento de A, logo $A \neq \emptyset$. Ainda, como X é limitado superiormente, $B \neq \emptyset$.

Para verificar (iv), sejam $\alpha \in A$ e $\beta \in B$. Assim, existe $x \in X$ tal que $\alpha < x$. Como $\beta \geq x$, obtemos $\beta > \alpha$.

Pelo corolário 5.2.15, ou A possui máximo, ou B possui mínimo. Vamos mostrar que a primeira alternativa não pode ocorrer, de onde decorrerá que B possui mínimo, que é a tese do teorema.

Tomemos, então, α arbitrário em A. Existe $x \in X$ tal que $\alpha < x$. Consideremos α' tal que $\alpha < \alpha' < x$. Como $\alpha' < x$, então $\alpha' \in A$ e é maior do que α, ou seja, nenhum elemento de A é maior do que os demais, como queríamos verificar. □

O teorema seguinte mostra que $\mathbb{R}$, como $\mathbb{Q}$, é um corpo arquimediano (reveja o Exercício 83).

Teorema 5.2.17. *O conjunto* $\mathbb{N}$ *dos naturais é ilimitado em* $\mathbb{R}$.

Demonstração. Suponhamos $\mathbb{N}$ limitado superiormente em $\mathbb{R}$ e seja $\alpha = \sup \mathbb{N}$. Assim, $\alpha \geq n$, para todo $n \in \mathbb{N}$. Como $n+1 \in \mathbb{N}$, para todo $n \in \mathbb{N}$, então $n+1 \leq \alpha$, para todo $n \in \mathbb{N}$, de onde obtemos $\alpha - 1$ como cota superior para $n \in \mathbb{N}$, menor do que o $\sup \mathbb{N}$, uma contradição. □

Exemplo 5.2.3. Como uma aplicação do que acabamos de estudar, vamos mostrar que existe um único número real positivo cujo quadrado é 2, isto é, a equação $x^2 = 2$ tem uma única solução real positiva (que já sabemos não ser racional). Tal solução se denota por $\sqrt{2}$. Como $\alpha^2 = (-\alpha)^2$, para todo $\alpha \in \mathbb{R}$, então $-\sqrt{2}$ também é solução da equação acima (e não há outras soluções! Por quê?).

Seja $X = \{x \in \mathbb{R}_+^* \mid x^2 < 2\}$. É claro que $X \neq \emptyset$. X é limitado superiormente, por exemplo, pelo número 3. De fato, $3 > x > 0$ equivale a $3^2 > x^2$, que é verdadeira para $x \in X$, pois, para esses números, $x^2 < 2$.

Pelo teorema anterior, X possui supremo, digamos, s. Mostremos que $s^2 = 2$, por exclusão dos casos $s^2 < 2$ e $s^2 > 2$, de onde seguirá a afirmação.

Suponhamos $s^2 < 2$. Como $\mathbb{R}$ é arquimediano , podemos argumentar como na demonstração do Teorema 5.1.3, e tomarmos h real positivo menor do que $\min\left\{1, \dfrac{2-s^2}{2s+1}\right\}$. Obtemos:

$$(s+h)^2 = s^2 + 2sh + h^2 < s^2 + 2sh + h = s^2 + h(2s+1) < s^2 + \frac{2-s^2}{2s+1}\cdot(2s+1) = 2,$$

isto é, $(s+h)^2 < 2$; logo $s+h \in X$, contradizendo o fato de que s é cota superior de X.

Suponhamos agora $s^2 > 2$. Como na demonstração do Teorema 5.1.3, se tomarmos h real positivo tal que $0 < h < \min\left\{1, \dfrac{2-s^2}{2s}\right\}$, obtemos:

$$(s-h)^2 = s^2 - 2sh + h^2 > s^2 - 2s\frac{2-s^2}{2s} + h^2 = 2 + h^2 > 2$$

isto é, $(s-h)^2 > 2$, logo $s - h > x$, $\forall x \in X$; contradizendo o fato de s ser a menor cota superior de X.

Está provado o que queríamos.

Antes de prosseguirmos, precisamos lembrar da definição de potência de base real e expoente inteiro.

Definição 5.2.10. Seja $a \in \mathbb{R}$ e $n \in \mathbb{N}$. Definimos a *potência* a^n recursivamente como sendo 1, se $n = 0$ e, para $n > 1$, como sendo $a \cdot a^{n-1}$. Finalmente, se $a \neq 0$,

definimos a^{-n} como sendo $(a^{-1})^n$.

Exercício 105. Se a e b são reais e n, m inteiros positivos, mostre, por indução, que:

1. $(ab)^n = a^n \cdot b^n$;

2. $a^n a^m = a^{n+m}$;

3. $(a^n)^m = a^{nm}$.

Estenda as propriedades anteriores para $n, m \in \mathbb{Z}$, lembrando que, para expoentes negativos, a base deve ser não nula.

Seguindo os mesmos passos do Exemplo 5.2.3, provaremos, mais geralmente, o seguinte fato:

Teorema 5.2.18. *Seja a um real positivo e $n > 0$ natural. Existe um único número real positivo que é solução da equação $x^n = a$.*

Demonstração. Seja $A = \{x \in \mathbb{R}_+^* \mid x^n < a\}$. Mostremos, como no exemplo anterior, que A é não vazio e é limitado superiormente, portanto, admite supremo. De fato, a expressão $\frac{a}{a+1}$ é, obviamente positiva e menor do que ambos, 1 e a. Assim, $(\frac{a}{a+1})^n < \frac{a}{a+1} < a$, logo, $\frac{a}{a+1} \in A$ e, portanto, A é não vazio. Como cota superior para A, tem-se o número $a+1$. De fato, $a+1 > x$, para todo $x \in A$, equivale a $(a+1)^n > x^n$, para todo $x \in A$ (verifique essa equivalência). A última desigualdade é verdadeira, como resulta de: $x^n < a < a+1 < (a+1)^n$, para todo $x \in A$ (para a última desigualdade, use a desigualdade de Bernoulli: $(1+a)^n > 1+na > 1+a$). Concluímos que $a+1$ é cota superior de A. Seja então $\alpha = \sup A$. Mostraremos, como no exemplo anterior, que $\alpha^n = a$, por exclusão dos casos $\alpha^n < a$ e $\alpha^n > a$.

Suponhamos inicialmente $\alpha^n < a$. Vamos mostrar que existe h positivo e menor do que 1 tal que $(\alpha + h)^n < a$, contrariando o fato de que α é cota superior de A. A análise do desenvolvimento da expressão $(\alpha + h)^n$ mostrará a existência de um tal h. Trata-se do chamado *desenvolvimento do binômio de Newton* (Veja [18] para uma demonstração desse desenvolvimento usando indução), segundo o qual tem-se:

$$(\alpha + h)^n = \alpha^n + \tbinom{n}{1}\alpha^{n-1}h + \tbinom{n}{2}\alpha^{n-2}h^2 + \cdots + \tbinom{n}{n-1}\alpha h^{n-1} + h^n.$$

Como $0 < h < 1$, a expressão acima fica menor do que

$$\alpha^n + h\left[\tbinom{n}{1}\alpha^{n-1} + \tbinom{n}{2}\alpha^{n-2} + \cdots + 1\right] = \alpha^n + h\left[(\alpha + 1)^n - \alpha^n\right].$$

Para que essa expressão fique menor do que a, deve-se ter $h < \dfrac{a - \alpha^n}{(\alpha + 1)^n - \alpha^n}$, o que é possível porque, sendo a última expressão positiva, basta tomar h como sendo ela vezes $\frac{1}{2}$. (Veja o Exercício 76.6 e estenda-o para $\mathbb{R}$ ou use o fato de que $\mathbb{R}$ é arquimediano.)

Suponhamos agora $\alpha^n > a$ e busquemos k positivo e menor do que 1 tal que $\alpha - k$ ainda satisfaça $(\alpha - k)^n > a$, de onde segue que $\alpha - k$ é cota superior de A menor do que $\sup A$, um absurdo. Temos, novamente, pela fórmula do binômio de Newton:

$$\begin{aligned}
(\alpha - k)^n &= \alpha^n - \binom{n}{1}\alpha^{n-1}k + \binom{n}{2}\alpha^{n-2}k^2 + \cdots + (-1)^n\binom{n}{n}\alpha k^n \\
&= \alpha^n - k\left[\binom{n}{1}\alpha^{n-1} - \binom{n}{2}\alpha^{n-2}k^2 + \cdots - (-1)^n\binom{n}{n}k^{n-1}\right] \\
&> \alpha^n - k\left[\binom{n}{1}\alpha^{n-1} + \binom{n}{2}\alpha^{n-2}k^2 + \cdots + \binom{n}{n}k^{n-1}\right] \\
&> \alpha^n - k\left[\binom{n}{1}\alpha^{n-1} + \binom{n}{2}\alpha^{n-2} + \cdots + \binom{n}{n}\right] \\
&= \alpha^n - k\left[(\alpha + 1)^n - \alpha^n\right], \qquad (5.1)
\end{aligned}$$

que fica maior do que a se $k < \dfrac{\alpha^n - a}{(\alpha+1)^n - \alpha^n}$. Pelas mesmas razões ao final do primeiro caso, um tal k real existe.

Concluímos, como queríamos, que α^n deve ser igual a a. A demonstração da unicidade de uma tal solução positiva é um exercício para o leitor (use a fatoração: $x^n - y^n = (x-y)\cdot(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \ldots + x^2y^{n-1} + xy^{n-2} + y^{n-1})$). □

Definição 5.2.11. Dado um número real positivo a, o único número real positivo que é solução da equação $x^n = a$, estabelecido pelo teorema anterior, chama-se *raiz n-ésima de a* e é denotado por $\sqrt[n]{a}$ ou por $a^{\frac{1}{n}}$. A raiz n-ésima de a permite que se defina expoente racional do seguinte modo: se m e n são inteiros positivos, $a^{\frac{m}{n}} = (a^{\frac{1}{n}})^m$ e, como para expoentes inteiros, $a^{-\frac{m}{n}} = (a^{-1})^{\frac{m}{n}}$. O tratamento de expoentes irracionais é considerado de forma rigorosa no estudo de funções exponenciais reais, o que costuma ser feito nos cursos de Cálculo Diferencial e Integral ou de Análise Matemática.

Exercício 106. Se a e b são reais positivos, n inteiro positivo e r, s racionais positivos, mostre que:

1. $(ab)^{\frac{1}{n}} = a^{\frac{1}{n}} \cdot b^{\frac{1}{n}}$;
2. $a^r a^s = a^{r+s}$;
3. $(a^r)^s = a^{rs}$;
4. $(ab)^r = a^r b^s$.

Exercício 107. Com o auxílio das propriedades acima, mostre que se $a > 1$ em $\mathbb{R}$ e $r > s > 0$ em $\mathbb{Q}$, então $a^r > a^s$.

Exercício 108. Mostre que se $a \in \mathbb{R}_+^*$ e $r \in \mathbb{Q}_+^*$, então $a > 1$ se, e somente se $a^r > 1$.

Exemplo 5.2.4. Utilizando os resultados contidos nos exercícios acima, mostraremos agora que o conjunto $A = \{x \in \mathbb{Q}_+^* \mid 10^x < 15\}$ é não vazio, limitado superiormente e que seu supremo, digamos, s, é um número irracional. Esse supremo denota-se por $\log_{10} 15$. No exercício seguinte, atribuiremos, de maneira natural, um significado a 10^s, segundo o qual teremos $10^s = 15$. Vamos aos detalhes. Claro que A é não vazio, pois $1 \in A$. Mostremos que A é limitado superiormente por 2. De fato, as desigualdades $2 > x > 0$ equivalem, pelo Exercício 107, a $10^2 > 10^x > 1$, que é verdadeira para todo $x \in A$, pois, para tais x, $10^x < 15 < 10^2$. Seja $s = \sup A$. Vamos mostrar que $s \notin \mathbb{Q}$ do seguinte modo: sob a hipótese de s pertencer a $\mathbb{Q}$, 10^s não poderá ser menor, nem maior e nem igual a 15. Já sabemos, do Exercício 90, que 10^x não pode ser 15 para nenhum expoente racional x. Excluiremos, um a um, os outros dois casos.

i) Suponhamos $10^s < 15$. Vamos encontrar $h \in \mathbb{Q}_+^*$ tal que $10^{s+h} < 15$, de onde decorrerá que $s + h \in A$, contrariando $s = \sup A$. A condição exigida sobre h equivale a $10^h < 15 \cdot 10^{-s}$, este último, maior do que 1, digamos, $1 + u$, $u > 0$. Busquemos um h da forma $\dfrac{1}{n}$, $n \in \mathbb{N}$, de modo que $1 < 10^{\frac{1}{n}} < 1 + u$, o que, pelo Exercício 107, equivale a $1 < 10 < (1+u)^n$. Mas, pela Desigualdade de Bernoulli (veja Exercício 85), $(1+u)^n > 1 + nu$, que, por ser $u > 0$, fica arbitrariamente grande, para n adequadamente grande. Um tal n produz o $h = \dfrac{1}{n}$ que desejamos.

ii) A suposição de que $10^s > 15$ é descartada de modo análogo ao caso que acabamos de estudar e o leitor deve trabalhá-la como exercício.

Exercício 109. Sejam A e $s = \log_{10} 15$, como no exemplo anterior. Definimos 10^s como sendo o supremo do conjunto $\{10^x \mid x \in A\}$. Mostre que $10^s = 15$.

Exercício 110. Com argumentos análogos aos utilizados no exercício e exemplo anteriores, defina $\log_8 15$ e $8^{\log_8 15}$ de modo que essa última expressão seja igual a 15.

Exercício 111. Generalize as ideias contidas nos exercícios anteriores para definir $\log_b a$, para b e a reais positivos, com $b \neq 1$. Além disso, se $\log_b a$ for irracional, defina, para c real positivo, $c^{\log_b a}$, de modo que $b^{\log_b a}$ seja igual a a.

Exercício 112. Sejam A e B subconjuntos não vazios de $\mathbb{R}$, limitados superiormente. Definimos $A+B$ como sendo o conjunto $\{x+y \mid x \in A \text{ e } y \in B\}$. Mostre que $A+B$ é limitado superiormente e que $\sup\,(A+B) = \sup A + \sup B$. Enuncie e prove resultado análogo para A e B não vazios e limitados inferiormente.

Exercício 113. Explicite os cortes correspondentes aos seguintes números reais:

1) 3 2) $-\frac{1}{3}$ 3) $\sqrt{3}$ 4) $\sqrt[5]{3}$ 5) $\sqrt{2}+\sqrt{3}$ 6) $\sqrt{2}\sqrt{8}$ 7) $\log_2 10$ 8) $\log_2 8$

Exercício 114. Demonstre as afirmações seguintes:

1. a soma e o produto de dois números irracionais pode ser racional;
2. a soma de um irracional com um racional é irracional.

Exercício 115. É comum vermos nos livros de matemática, nos mais variados níveis, exercícios com os enunciados seguintes:

1. mostre que a equação $x^2 = 2$ não admite solução racional;
2. mostre que $\sqrt{2} \notin \mathbb{Q}$;
3. mostre que $\sqrt{2}$ é irracional.

Esperando-se que o leitor resolva rigorosamente esses exercícios, diga que conteúdo matemático ele deverá utilizar para demonstrar cada um deles.

O Teorema 5.1.3 e o Exemplo 5.2.4 expressam, no presente contexto, o fato de que há conjuntos não vazios de racionais, limitados superiormente, que não admitem supremo racional, por exemplo, $A = \{x \in \mathbb{Q}_+ \mid x^2 < 2\}$ (conforme o item 3 do Exercício 116 abaixo). No entanto, pelo Teorema 5.2.16, A tem supremo, se considerado como subconjunto de $\mathbb{R}$, a saber, $\sqrt{2}$ (o que se prova de modo similar ao exemplo anterior, com o cuidado de, através do Teorema 5.2.13, tomar h racional).

Exercício 116. Mostre que:

1. todo subconjunto não vazio de reais, limitado inferiormente, possui ínfimo;

2. se X e Y são subconjuntos não vazios limitados de $\mathbb{R}$ e se $X \subset Y$, então $\inf Y \leq \inf X$ e $\sup X \leq \sup Y$;

3. o conjunto $A = \{x \in \mathbb{Q}_+ \mid x^2 < 2\}$ não possui supremo em $\mathbb{Q}$.

5.3 Representação decimal dos números reais

No Capítulo 2, dissemos que utilizaríamos o sistema de numeração indo-arábico para representar os números naturais, portanto os inteiros e racionais escritos na forma de fração. Esse sistema é dito *posicional de base dez* por razões conhecidas desde o ensino básico de matemática. Na verdade, qualquer número natural b maior do que 1 pode ser a base de um sistema posicional para a representação dos números inteiros, de modo análogo ao sistema decimal (consulte [18] para uma demonstração rigorosa desse fato). Por exemplo, o sistema binário (base dois) é de fundamental importância em computação. Claro que o sistema decimal se consolidou ao longo

da nossa história devido às dez peças de nossa ferramenta mais antiga de contagem: os dedos das mãos. Certamente, se tivéssemos três dedos em cada mão, nosso sistema de numeração seria, naturalmente, o de base seis.

Assumindo conhecida a representação dos inteiros em base dez, vamos estudar a representação decimal dos números reais, isto é, em que se baseia a escrita de números reais na forma 1,7; -3,43; 3,14159...; 0,7777... etc.

Exercício 117. Dado um número real não negativo α, mostre que existe um número natural máximo, n_0, que é menor do que ou igual a α. Mostre ainda que $0 \leq \alpha - n_0 < 1$.
(*Sugestão*: considere o conjunto dos números naturais maiores do que α e use o Princípio da Boa Ordem.)

No teorema a seguir, estudaremos a representação decimal dos números reais não negativos menores do que 1, a partir da qual a representação decimal dos demais números reais será automática, com o auxílio do exercício acima e do sinal "-".

Teorema 5.3.1. ***(Representação decimal dos números reais)***
i) A cada número real α, não negativo e menor do que 1, corresponde uma única sequência de dígitos $(n_k)_{k\in\mathbb{N}^*}$, satisfazendo:
a) $0 \leq n_k \leq 9$, para todo $k \in \mathbb{N}^*$;
b) $(n_k)_{k\in\mathbb{N}^*}$ não possui infinitos dígitos consecutivos iguais a 9; e
c) definindo, para cada $k \in \mathbb{N}^*$, S_k como a soma $\dfrac{n_1}{10} + \cdots + \dfrac{n_k}{10^k}$, α será o supremo do conjunto $S = \{S_k \mid k \in \mathbb{N}^*\}$.
ii) Reciprocamente, a cada sequência de dígitos $(n_k)_{k\in\mathbb{N}^*}$, satisfazendo (a) e (b) acima, e definindo S_k como em (c), corresponde um único número real α, não

negativo e menor do que 1, que é o supremo do conjunto limitado superiormente $S = \{S_k \mid k \in \mathbb{N}^*\}$.

Demonstração. i) Dado α como no enunciado, seja n_1 o maior natural tal que $\frac{n_1}{10} \leq \alpha$. Observe dois fatos importantes neste ponto: que um tal n_1 existe e que $0 \leq n_1 \leq 9$. Prove ambos!

Se $\frac{n_1}{10} = \alpha$, associamos a α a sequência $(n_1, 0, 0, 0\ldots)$. Se $\frac{n_1}{10} < \alpha$, seja n_2 o maior número natural tal que $\frac{n_1}{10} + \frac{n_2}{10^2} \leq \alpha$. Novamente, tal n_2 existe e satisfaz $0 \leq n_2 \leq 9$, caso contrário contradir-se-ia a forma com que n_1 fora tomado (verifique).

Se $\frac{n_1}{10} + \frac{n_2}{10^2} = \alpha$, associamos a α a sequência $(n_1, n_2, 0, 0, 0\ldots)$. Se $\frac{n_1}{10} + \frac{n_2}{10^2} < \alpha$, tomamos n_3 como o maior natural satisfazendo $\frac{n_1}{10} + \frac{n_2}{10^2} + \frac{n_3}{10^3} \leq \alpha$, que, como nos casos anteriores, satisfaz $0 \leq n_3 \leq 9$.

Obtidos, dessa forma, $n_1, n_2, \ldots, n_{k-1}$, obtemos n_k como o maior inteiro tal que $\frac{n_1}{10} + \cdots + \frac{n_k}{10^k} \leq \alpha$, com n_k satisfazendo, necessariamente, $0 \leq n_k \leq 9$.

A α, associamos a sequência $(n_k)_{k \in \mathbb{N}^*}$ determinada na construção acima.

O fato de que esta sequência não possui infinitos noves consecutivos será estabelecido no Exercício 123

Consideremos agora S e S_k como na primeira parte do teorema e verifiquemos que, de fato, $\alpha = \sup S_k$. α é cota superior de S, por construção. Seja β um real positivo menor do que α. Mostremos que β não pode ser cota superior de S. Como $\mathbb{R}$ é arquimediano (Teorema 5.2.17), existe $k \in \mathbb{N}$ tal que $\frac{1}{10^k} < \alpha - \beta$. Temos: $\alpha - S_k < \frac{1}{10^k} < \alpha - \beta$, de onde segue que $\beta < S_k$, como queríamos.

ii) Reciprocamente, dada uma sequência $(n_k)_{k \in \mathbb{N}^*}$, $(0 \leq n_k \leq 9)$, para todo k, como acima, construímos os conjuntos S_k e S do enunciado. S é limitado superiormente pela *série geométrica* $\frac{9}{10} + \frac{9}{10^2} + \cdots + \frac{9}{10^k} + \cdots$, que *converge* para 1 (Veja Exer-

cícios 119 e 120 adiante e, também, [11] para maiores detalhes sobre séries numéricas). Assim, $\alpha = \sup S$ é o número real associado à sequência $(n_k)_{k\in\mathbb{N}^*}$. $\square$

Definição 5.3.1. i) Dado um número real α, com $0 \leq \alpha < 1$, seja $(n_k)_{k\in\mathbb{N}^*}$ a sequência de dígitos correspondente a α, sem infinitos noves consecutivos, construída na primeira parte do teorema acima. A *representação decimal de* α se define como sendo a expressão $0,n_1n_2n_3n_4\ldots$. Se $n_k \neq 0$ e $n_l = 0$, para todo $l > k$, convenciona-se representar $0,n_1n_2n_3n_4\ldots$ por $0,n_1n_2n_3n_4\ldots n_k$, que será dita *representação decimal finita de* α.

ii) Se $\alpha \geq 1$, seja n_0 o maior natural que é menor do que ou igual a α, dado no Exercício 117. Seja $0,n_1n_2n_3n_4\ldots n_k\ldots$ a representação decimal de $\alpha - n_0$ definida em (i). Definimos a representação decimal de α como sendo a expressão $n_0,n_1n_2n_3n_4\ldots n_k\ldots$.

iii) Se $\alpha < 0$, definimos sua representação decimal como sendo $-r$, onde r é a representação decimal de $-\alpha$.

Exercício 118. Escreva a representação decimal dos seguintes números reais:
1. $\sqrt{2}$ (com três dígitos após a vírgula); 2. $\frac{3}{5}$; 3. $\frac{20}{3}$; 4. $-\frac{3}{4}$.

Exercício 119. Determine o número real cuja representação decimal é:

1. $0,4444\ldots$ (Utilize aqui o fato de que a série geométrica $\sum_{n=1}^{\infty} aq^n$, com $a > 0$ e $0 < q < 1$, converge para $\frac{a}{1-q}$. Isso significa que o conjunto $\{a + aq + aq^2 + \ldots + aq^n \mid k \in \mathbb{N}\}$ possui supremo $\frac{a}{1-q}$.);

2. $-2,121212\ldots$;

3. $1,3121212\ldots$;

4. $-3,7$.

Nossas representações decimais não consideram, então, expressões com infinitos noves consecutivos, como $0,99999...$, $2,79999...$ etc. É possível, no entanto, atribuir a elas um significado similar ao das expressões sem infinitos noves consecutivos. Abordemos inicialmente a expressão $0,99999...$. Estendendo o que vimos para representações sem infinitos noves sucessivos, o número real α a ela associado deve ser o supremo do conjunto $S = \{S_k \mid k \in \mathbb{N}^*\}$, onde $S_k = \frac{9}{10} + \frac{9}{10^2} + \cdots + \frac{9}{10^k}$, que é, conforme vimos na demonstração do teorema anterior, o número real 1. Por outro lado, a representação decimal de 1 é, pela definição acima, 1,00000..., que convencionamos representar pelo próprio símbolo 1. Consequentemente, considerando expressões com infinitos noves consecutivos como representações decimais, tem-se como resultado que elas representam também números reais com representação decimal finita e, reciprocamente, qualquer representação decimal finita, diferente da do número 0, admite uma representação decimal com infinitos noves consecutivos nos termos acima. Confirme essas afirmações no exercício seguinte.

Exercício 120. Mostre que a representação decimal $2,79999...$ também representa o número (representado por) $2,8$. Qual a representação decimal com infinitos noves de 0,47? E de 2,99? Generalize.

Os três últimos exercícios apontam para o fato de que representações decimais finitas ou *periódicas* (aquelas que contêm a repetição sucessiva de um bloco de dígitos) correspondem a números racionais. (Prove isso como exercício.)

Reciprocamente, pode-se provar que todo número racional possui representação decimal finita ou periódica. (Para uma demonstração rigorosa desse fato, consulte,

por exemplo, [11]. Veja também os dois exercícios seguintes.) Assim, representações como $0,101001000100001\ldots$ e $4,1234567891011\ldots$ correspondem a números irracionais.

Exercício 121. Mostre que uma fração irredutível possui representação decimal finita se, e somente se, seu denominador for divisor de uma potência de 10.

Exercício 122. Explique porque $\frac{4}{3}$ possui representação decimal periódica. Idem para $\frac{8}{11}$ e $\frac{4}{7}$.

Exercício 123. Dado um real α, não negativo e menor do que 1, mostre que a sequência associada a α, construída na primeira parte do Teorema 5.3.1, não conduz a infinitos noves sucessivos.

5.4 $\mathbb{R}$ não é enumerável

A representação decimal dos números reais permite demonstrar que $\mathbb{R}$ não é enumerável. É o que faremos a seguir.

Exercício 124. Com o auxílio do Lema 4.3.4, mostre que todo subconjunto infinito de um conjunto enumerável é enumerável.

Lema 5.4.1. *O intervalo* $I =]0,1[$ *não é enumerável.*

Demonstração. Mostraremos que, qualquer que seja a enumeração estabelecida para elementos de I, sempre existirá um elemento de I não considerado na dada enumeração. Em outras palavras: qualquer subconjunto enumerável de I é diferente de I, de onde obteremos que I não pode ser enumerável. De fato, seja I' um

conjunto enumerável constituído de elementos de I que, portanto, pode ser escrito na forma $I' = \{x_0, x_1, x_2, \ldots\}$, onde, para cada $n \in \mathbb{N}$, x_n representa a imagem de n por uma certa bijeção de $\mathbb{N}$ em I'. Vamos representar cada elemento de I' pela sua representação decimal dada acima, sem infinitos noves consecutivos, e dispô-las na forma de uma "matriz infinita", assim:

$$\begin{aligned} x_0 &= 0, x_{00}x_{01}x_{02}\ldots \\ x_1 &= 0, x_{10}x_{11}x_{12}\ldots \\ x_2 &= 0, x_{20}x_{21}x_{22}\ldots \\ &\vdots \\ x_k &= 0, x_{k0}x_{k1}x_{k2}\ldots \\ &\vdots \end{aligned}$$

Vamos construir agora um número real $x \in I$, diferente de todos os elementos de I' através da seguinte representação decimal: $0, a_0a_1a_2a_3\ldots$, onde, para cada $n \in \mathbb{N}$, o dígito decimal a_n dessa representação é diferente de 9, de 0 e do dígito decimal x_{nn} da representação de x_n. Pela correspondência bijetora estabelecida acima entre números reais e representações decimais sem infinitos noves, a representação decimal $0, a_0a_1a_2a_3a_4\ldots$ corresponde a um único número real de I que é diferente de todos os elementos de I', como queríamos. Este belo e simples argumento também se deve a Cantor e, por razões óbvias, chama-se *método diagonal de Cantor*. □

Teorema 5.4.2. *O conjunto dos números reais é não enumerável.*

Demonstração. O subconjunto I de $\mathbb{R}$, dado no lema anterior é não enumerável e, portanto, pelo Exercício 124, $\mathbb{R}$ não pode ser enumerável. □

Os resultados seguintes exibem bijeções entre o intervalo I do lema anterior e subconjuntos notáveis de $\mathbb{R}$ e de $\mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R}$ (n fatores, $n \geq 2$), que se denota por $\mathbb{R}^n$. Geometricamente, esse fato mostra, em particular, que o segmento de reta aberto que representa I é equipotente a uma reta (que representa $\mathbb{R}$), ao plano (que representa $\mathbb{R}^2$), e ao espaço tridimensional (que representa $\mathbb{R}^3$).

Exercício 125. Mostre que a função $f : \mathbb{R} \to I$ dada por $f(x) = \frac{1}{2}\left(1 + \frac{x}{1+|x|}\right)$ é bijetora.

No exercício seguinte, considere, para os números do domínio da função, a representação decimal com infinitos noves consecutivos, em vez de decimais exatas. Seja $J = [0,1] = \{x \in \mathbb{R} \mid 0 \leq x \leq 1\}$.

Exercício 126. Usando a representação decimal dos números reais, mostre que a função $f : J \to J \times J$ $(= J^2)$, dada por $f(0, a_0a_1a_2a_3a_4\ldots) = (0, a_0a_2a_4a_6a_8\cdots, 0, a_1a_3a_5a_7a_9\cdots)$ é sobrejetora. Exiba uma sobrejeção de J sobre J^3. Generalize.

Exercício 127. Exiba uma sobrejeção de J^2 sobre J. Exiba uma sobrejeção de J^n sobre J, $n \geq 3$.

O importante Teorema de Schröder-Bernstein (veja [17], [30]) afirma que se A e B são conjuntos e existem sobrejeções $f : A \to B$ e $g : B \to A$, então A e B são equipotentes, isto é, existe uma bijeção entre esses conjuntos. (A mesma conclusão é obtida se considerarmos f e g funções injetoras ao invés de sobrejetoras.) Utilize este resultado e os exercícios anteriores para concluir a proposição seguinte.

Proposição 5.4.3. *Existe uma bijeção entre* $[0,1]$ *e* $[0,1]^n$ *(*$n \geq 2$*).*

Exercício 128. Mostre que a função $f :]0,1[\to]a,b[$ dada por $f(x) = a + (b-a)x$ é bijetora. Assim, qualquer intervalo aberto é equipotente ao intervalo $]0,1[$.

Lema 5.4.4. *Um intervalo do tipo* $[a,b]$ *é equipotente ao intervalo do tipo* $[a,b[$.

Demonstração. Pelo exercício anterior, $]a,b[$ é não enumerável, logo o são os intervalos do enunciado. Seja $A = \{a_1, a_2, \cdots\}$ um subconjunto enumerável de $[a,b[$. Considere a função f de $[a,b]$ em $[a,b[$ dada por $f(x) = x$, se $x \in [a,b[\setminus A$, $f(a_n) = a_{n+1}$, para $n \in \mathbb{N}^*$ e $f(b) = a_1$. Tal função é bijetora (certifique-se desse fato). $\square$

Exercício 129. Mostre que os intervalos $]a,b[$ e $[a,b]$ são equipotentes. Em particular o são os intervalos I e J dos exercícios anteriores.

Usando os resultados anteriores e lembrando que a composição de bijeções é uma bijeção, demonstre a proposição a seguir.

Proposição 5.4.5. *Qualquer intervalo de números reais (por menor que seja sua amplitude) é equipotente a* $\mathbb{R}^n$*, para todo* $n \geq 1$.

Proposição 5.4.6. *Os conjuntos* $\mathbb{R}$ *e* $\mathcal{P}(\mathbb{N})$ *são equipotentes.*

Demonstração. Novamente, utilizaremos o Teorema de Schröder-Bernstein acima mencionado, juntamente com outros resultados já provados, da seguinte forma: mostraremos que existe uma função injetora $\varphi : \mathbb{R} \to \mathcal{P}(\mathbb{Q})$ e uma função injetora $f : \mathcal{P}(\mathbb{N}) \to \mathbb{R}$. Como $\mathbb{Q}$ e $\mathbb{N}$ são equipotentes, assim o serão os conjuntos $\mathcal{P}(\mathbb{Q})$ e $\mathcal{P}(\mathbb{N})$, isto é, existe uma bijeção $\psi : \mathcal{P}(\mathbb{Q}) \to \mathcal{P}(\mathbb{N})$. A função $g = \psi \circ \varphi : \mathbb{R} \to \mathcal{P}(\mathbb{N})$ será, portanto, injetora. Das injetividades de f e de g, concluímos pelo Teorema de Schröder-Bernstein, a tese da proposição. Vamos então às definições das funções

injetoras φ e f acima mencionadas. Definimos $\varphi : \mathbb{R} \longrightarrow \mathcal{P}(\mathbb{Q})$ do seguinte modo: a cada $a \in \mathbb{R}$, $\varphi(a) = \{x \in \mathbb{Q} \mid x < a\}$. Mostremos que φ é injetora. De fato, sejam a e b reais com $a < b$. Pelo Teorema 5.2.13, existe um número racional $r \in]a,b[$. Como $r \in \varphi(b) \setminus \varphi(a)$, então $\varphi(b) \neq \varphi(a)$.

Para definirmos $f : \mathcal{P}(\mathbb{N}) \longrightarrow \mathbb{R}$, seja $A \in \mathcal{P}(\mathbb{N})$ e consideremos a *função característica de A*, $\chi_A : \mathbb{N} \longrightarrow \{0,1\}$, dada por $\chi_A(n) = 1$, se $n \in A$, e $\chi_A(n) = 0$, se $n \in \mathbb{N} \setminus A$. Observe que existe uma função característica para cada subconjunto de $\mathbb{N}$ e, vice-versa, a cada função $\chi : \mathbb{N} \longrightarrow \{0,1\}$, corresponde o subconjunto de $\mathbb{N}$ que é a pré-imagem de 1, isto é, o conjunto $\{n \in \mathbb{N} \mid \chi(n) = 1\}$. Dessa forma, elas *caracterizam* os subconjuntos de $\mathbb{N}$, daí seu nome. Com o auxílio dessa função característica, definimos $f(A)$ como sendo o número real cuja representação decimal será $0,\chi_A(0)\chi_A(1)\chi_A(2)\chi_A(3)\ldots$. O leitor deve verificar que f é injetora, isto é, se $A \neq B$, então os números reais de representações decimais $0,\chi_A(0)\chi_A(1)\chi_A(2)\chi_A(3)\ldots$ e $0,\chi_B(0)\chi_B(1)\chi_B(2)\chi_B(3)\ldots$ são diferentes. (Observe ainda que os números reais que possuem as representações decimais definidas acima pertencem ao intervalo $[0,\frac{1}{9}]$.)

□

6

Números complexos

No Ensino Médio, os números complexos são introduzidos a partir da chamada "unidade imaginária", i, com a propriedade de que $i^2 = -1$. Eles são definidos, então, como expressões da forma $a + bi$, onde $a, b \in \mathbb{R}$, sujeitas às regras operacionais conhecidas dos números reais. Assim, por exemplo, $(3 + 5i) \cdot (7 - 2i) = 21 - 6i + 35i - 10i^2 = 21 + 29i + 10 = 31 + 29i$. Ou seja, manipulam-se tais expressões como expressões algébricas reais, sob a condição extra de que $i^2 = -1$.

Novamente, do ponto de vista do rigor matemático, é necessário justificar cuidadosamente a origem de um tal número i.

6.1 Construção dos complexos e sua aritmética

A construção rigorosa dos números complexos a partir dos números reais é mais simples do que todas as construções que realizamos até agora.

No Ensino Médio, aprendemos que dois números complexos, $a + bi$ e $c + di$, são iguais apenas quando $a = c$ e $b = d$, o que nos lembra a igualdade entre os pares ordenados (a, b) e (c, d). É este o ponto de partida para a construção dos complexos.

Lembramos ainda, do Ensino Médio, que:

$$(a+bi)+(c+di)=(a,c)+(b+d)i$$

e que

$$(a+bi)\cdot(c+di)=(ac-bd)+(ad+bc)i.$$

Se admitíssemos um número complexo como sendo um par ordenado de números reais, portanto, sem mencionar o símbolo i, poderíamos definir as operações acima do seguinte modo:

$$(a,b)+(c,d)=(a+c,b+d) \qquad \text{e} \qquad (a,b)\cdot(c,d)=(ac-bd,ad+bc)\cdot$$

Formalmente, então, temos a definição a seguir:

Definição 6.1.1. Consideremos o conjunto $\mathbb{R}\times\mathbb{R}=\mathbb{R}^2$ e nele definamos a adição e a multiplicação como acima. O conjunto $\mathbb{R}^2$, dotado com essas operações, será denominado *conjunto dos números complexos* e denotado por $\mathbb{C}$.

Teorema 6.1.1. *As operações em $\mathbb{C}$ têm as seguintes propriedades: a adição e a multiplicação são comutativas, associativas e têm elemento neutro: $(0,0)$ para a adição e $(1,0)$ para a multiplicação. Além disso, dado $(a,b)\in\mathbb{C}$, seu simétrico existe, $-(a,b)$, e é $(-a,-b)$ e, se $(a,b)\neq(0,0)$, seu inverso existe, $(a,b)^{-1}$, e é $\left(\frac{a}{a^2+b^2},\frac{-b}{a^2+b^2}\right)$. Finalmente, a multiplicação é distributiva em relação à adição.*

Demonstração. Exercício. □

Exercício 130. Encontre o inverso de $\left(\frac{1}{3},-2\right)$.

Vamos agora imergir $\mathbb{R}$ em $\mathbb{C}$ de forma natural. Observe inicialmente que um número complexo arbitrário (a,b) pode ser escrito como $(a,b) = (a,0) + (b,0)(0,1)$, ou seja, utilizando-se apenas pares ordenados com segunda coordenada nula, $(a,0)$ e $(b,0)$, e o número complexo especial $(0,1)$.

Considere agora a seguinte função:

$$k : \mathbb{R} \to \mathbb{C}, \qquad \text{dada por} \qquad k(x) = (x,0).$$

Teorema 6.1.2. *A função k acima é injetora e preserva as operações de adição e de multiplicação, isto é, $k(x+y) = k(x) + k(y)$ e $k(xy) = k(x) \cdot k(y)$. Em particular, $\mathbb{C}$ é não enumerável.*

Demonstração. Exercício. □

De modo similar aos casos estudados anteriormente, aqui também temos em $\mathbb{C}$ uma cópia algébrica de $\mathbb{R}$, $k(\mathbb{R})$, o que nos permite identificar $\mathbb{R}$ com $k(\mathbb{R})$ e, portanto, considerar $\mathbb{R} \subset \mathbb{C}$.

Admitindo essa identificação e adotando o símbolo i para o número complexo $(0,1)$, a expressão para (a,b), que é igual a $(a,0) + (b,0)(0,1)$, pode ser escrita como $a + bi$, como fazíamos no Ensino Médio.

Note ainda que $i^2 = (0,1)^2 = (-1,0)$, que se identifica com o real -1!

Sob a notação acima, os complexos do tipo $a + bi$, com $b \neq 0$, chamam-se *números imaginários*, e, se além disso, $a = 0$, obtemos os *imaginários puros*. Essas denominações têm sua origem na resistência histórica em se admitir os complexos como números. Observe que o termo "*imaginários*" vem no sentido de contraposição a "*reais*".

6.2 $\mathbb{C}$ não é ordenável

Observe que as propriedades aritméticas de $\mathbb{C}$, dadas no Teorema 6.1.1, são as mesmas que as de $\mathbb{R}$ (que são as mesmas que as de $\mathbb{Q}$). Conforme mencionado no Capítulo 4, um conjunto, munido de duas operações que podemos continuar denotando por $+$ e $\cdot$, possuindo essas propriedades aritméticas chama-se *corpo*.

Apesar dessas semelhanças, há grandes diferenças entre os três corpos, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$. Os corpos $\mathbb{Q}$ e $\mathbb{R}$, como já tínhamos visto, são dotados de uma relação de ordem compatível com as suas operações e são, portanto, ambos *ordenados*, sendo $\mathbb{R}$ um *corpo ordenado completo* e $\mathbb{Q}$ um *corpo ordenado* não completo.

No exercício seguinte, pede-se para demonstrar que é impossível dotar $\mathbb{C}$ de uma relação de ordem compatível com as suas operações aritméticas. Intuitivamente, não temos como dizer se 3 é maior ou menor do que $3i$ ou do que $2+i$, por exemplo. Dessa forma, $\mathbb{C}$ é um corpo não ordenável. No entanto, $\mathbb{C}$ possui uma importante propriedade algébrica que $\mathbb{R}$ e $\mathbb{Q}$ não têm: o *Teorema Fundamental da Álgebra*, cuja demonstração foi a tese de doutoramento de Gauss, afirma que todo polinômio não constante com coeficientes complexos admite uma raiz em $\mathbb{C}$. (Para uma demonstração algébrica deste teorema, veja [9] e, para um elegante argumento elementar, veja [24].)

Exercício 131. Com o auxílio do Exercício 78, mostre que $\mathbb{C}$ *não é um corpo ordenável.*

Exercício 132. Com o auxílio do Teorema Fundamental da Álgebra e do *Teorema de D'Alembert* (veja [24]), mostre que todo polinômio *de grau* n, com coeficientes complexos, possui exatamente n raízes, contadas com suas *multiplicidades*.

Devido ao Teorema Fundamental da Álgebra, $\mathbb{C}$ diz-se um *corpo algebricamente fechado*. Notemos ainda que $\mathbb{Z}$ não é corpo, pois seus únicos elementos inversíveis são 1 e -1, conforme a Proposição 3.3.6. No entanto, $\mathbb{Z}$ possui todas as outras propriedades de corpo, além de uma relação de ordem que satisfaz o Princípio da Boa Ordem. Na linguagem algébrica, $\mathbb{Z}$ diz-se um *domínio de integridade bem ordenado*. Finalmente, $\mathbb{N}$ não possui nem a propriedade do elemento simétrico.

6.3 Números algébricos e transcendentes

As equações do tipo $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$, onde os coeficientes são números inteiros, são de grande importância em álgebra e denominam-se *equações algébricas*. Suas soluções complexas, conforme exercício acima, chamam-se *números algébricos*, sobre os quais há uma ampla e rica teoria (veja [29]). Os números reais que não podem ser obtidos como soluções de uma equação algébrica denominam-se *números transcendentes*. Assim, os números transcendentes são os reais que não são algébricos. Dessa forma, o conjunto dos números reais também é a união disjunta do conjunto dos números transcendentes com o conjunto dos números algébricos reais. (Em contextos mais gerais, qualquer número complexo que não é algébrico denomina-se também transcendente, mas, para simplificar a nomeclatura, reservaremos esse termo para os números reais que não são algébricos.)

Exercício 133. Mostre que os números $\sqrt{2}$, i, $1+i$ e $-\frac{3}{5}$ são algébricos. Mostre que todo número racional é algébrico, embora, obviamente, existam números algébricos irracionais e até imaginários.

Pode-se provar que as famosas constantes π e e são números irracionais trans-

cendentes (veja [12]). O curioso é que, num certo sentido, há em $\mathbb{R}$ "mais" números transcendentes do que algébricos. Mais precisamente, temos a seguinte situação: o conjunto dos números algébricos é enumerável (conforme provaremos adiante), logo o será o conjunto dos algébricos reais. O conjunto $\mathbb{R}$ é não enumerável (conforme Teorema 5.4.2), portanto o conjunto dos números transcendentes não pode ser enumerável, senão $\mathbb{R}$ o seria, como união de dois conjuntos enumeráveis (lembre-se do Exercício 72). Vamos então aos passos para a prova da enumerabilidade do conjunto dos números algébricos.

Primeiramente, observe que em um polinômio de grau n, $a_0 + a_1x^1 + a_2x^2 + \cdots + a_nx^n$, o que importa são seus coeficientes, e não o nome da indeterminada x, que poderia ser y, t, etc. Assim, um tal polinômio identifica-se naturalmente e univocamente com a *sequência quase nula* $(a_0, a_1, a_2, ..., a_n, 0, 0, 0...)$ constituída de seus coeficientes. A expressão "quase nula" deve-se ao fato de que a sequência em questão contém apenas um número finito de termos não nulos. E, claro, vice-versa, cada tal sequência determina, de modo único, um polinômio da forma acima.

Precisaremos agora dos fatos estabelecidos nos exercícios e lemas seguintes.

Exercício 134. Com um argumento análogo ao utilizado para provar que $\mathbb{Q}$ é enumerável, prove que o produto cartesiano $\mathbb{N} \times \mathbb{N}$ é enumerável.

Lema 6.3.1. *O produto cartesiano de dois conjuntos enumeráveis é enumerável.*

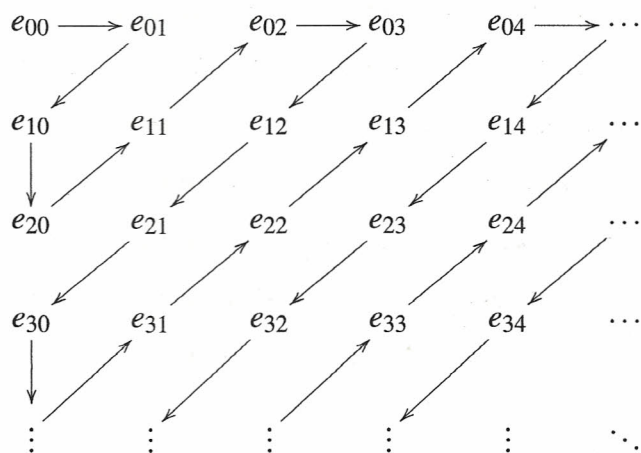
Demonstração. Sejam A e B dois conjuntos enumeráveis e $f : A \to \mathbb{N}$, $g : B \to \mathbb{N}$ bijeções. Definimos $h : A \times B \to \mathbb{N} \times \mathbb{N}$ por $h(x,y) = (f(x), g(y))$. A aplicação h é injetora (verifique) e tem como imagem um subconjunto infinito do conjunto

enumerável $\mathbb{N} \times \mathbb{N}$, logo, pelo exercício acima e pelo Exercício 124, $A \times B$ é enumerável. □

Exercício 135. Mostre, por indução, que o produto cartesiano de um número finito de conjuntos enumeráveis é enumerável.

Lema 6.3.2. *Seja* $(E_n)_{n\in\mathbb{N}}$ *uma família enumerável de conjuntos enumeráveis. A união* $E = \bigcup_{n\in\mathbb{N}} E_n$ *é enumerável.*

Demonstração. Para cada $j \in \mathbb{N}$, denotamos os elementos de E_j por $\{e_{j0}, e_{j1}, e_{j2}, \ldots\}$. Obtemos uma tabela "infinita" com o aspecto:

As setas na figura sugerem uma enumeração desses símbolos. Como, dentre eles, podem ocorrer repetições de elementos de E, E pode ser considerado um subconjunto infinito desses símbolos que é, pelo Exercício 124, enumerável. □

Observe que poderíamos provar que o produto cartesiano de dois conjuntos enu-

meráveis, A e B, é enumerável, como consequência do lema anterior, bastando para isso expressar $A \times B$ como $\bigcup_{a \in A}(\{a\} \times B)$.

Exercício 136. Mostre que a união enumerável de conjuntos finitos é finita ou enumerável.

Teorema 6.3.3. *O conjunto dos números algébricos é enumerável.*

Demonstração. Para cada $n \geq 1$, seja P_n o conjunto de todos os polinômios de grau n com coeficientes inteiros. Cada um desses polinômios identifica-se com uma (n+1)-upla de números inteiros $(a_0, a_1, a_2, \cdots, a_n)$, constituída pelos seus coeficientes. Essa (n+1)-upla é um elemento do produto cartesiano $\mathbb{Z} \times \mathbb{Z} \times ... \times \mathbb{Z}$ ($(n+1)$ fatores), que é enumerável, pelo Exercício 135. Por isso, P_n é enumerável. Seja $P_n = \{p_0, p_1, ...\}$ uma enumeração para P_n. Cada polinômio p_j de P_n possui, no máximo, n raízes complexas distintas, que compõem um conjunto finito, digamos, R_j. Assim, o conjunto de raízes obtidas dos membros de P_n é $\mathcal{R}_n = \bigcup_{j \in \mathbb{N}} R_j$, que é, pelo exercício anterior, enumerável. O conjunto dos números algébricos é precisamente a união (enumerável) de todos esses conjuntos enumeráveis, $\mathcal{R}_n$, que é, pelo Lema 6.3.2, enumerável. □

O teorema anterior mostra que os "responsáveis" pela não enumerabilidade de $\mathbb{R}$ são os números transcendentes. A demonstração desse fato, construída acima, ilustra um tipo de argumentação tipicamente matemática, que consiste em provar-se a existência de objetos (infinitos deles, no caso presente) sem construir qualquer um deles. De fato, provamos que o conjunto dos números transcendentes é infinito não enumerável, mas não apresentamos mais nenhum elemento desse conjunto

além de π e e! Os exercícios seguinte apresentam concretamente mais infinidade de transcendentes a partir de um transcendente dado.

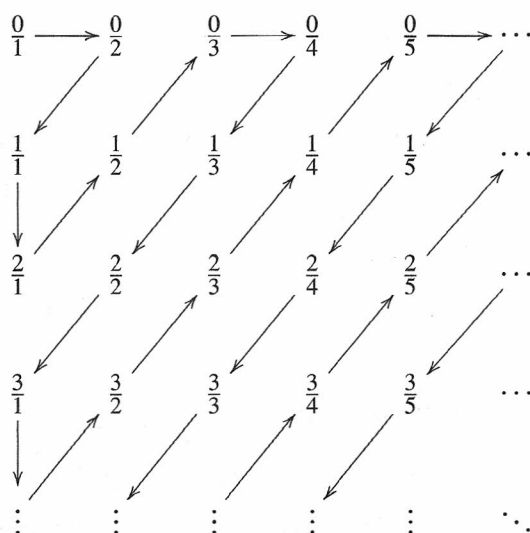
Exercício 137. Sejam t um número transcendente e n um natural positivo. Mostre que nt é transcendente. (*Sugestão*: suponha que nt fosse raiz de um polinômio com coeficientes inteiros e deduza que t também o seria.) Verifique que nt mantém-se transcendente mesmo se n for um racional não nulo qualquer.

Exercício 138. Nos cursos mais avançados de álgebra e de teoria dos números, prova-se que o conjunto $\mathcal{A}$ dos números algébricos é *fechado* para as operações de adição e de multiplicação (subtração e divisão) usuais de números complexos. Além disso, com essas operações, $\mathcal{A}$ é um corpo (um *subcorpo* de $\mathbb{C}$), denominado *corpo dos números algébricos* (veja, por exemplo, [9], [14], [29]). Use esse fato para mostrar que:

i) Se t é transcendente e a algébrico real não nulo, então ta é transcendente;

ii) Se t é transcendente e a algébrico real, então $t+a$ é transcendente;

iii) Verifique que o conjunto dos números transcendentes não é um corpo. Também não é corpo o conjunto dos números irracionais.

Exercício 139. Utilize um argumento análogo ao utilizado no Lema 6.3.2 para produzir outra demonstração de que $\mathbb{Q}$ é enumerável (veja o Teorema 4.3.7). Trabalhe na tabela de símbolos fracionários seguinte:

Tendo em vista as imersões que estudamos nos capítulos anteriores, podemos dizer que

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

Exercício 140. Construa um diagrama de conjuntos, cujo universo é o conjunto dos números complexos, destacando nele os subconjuntos dos números naturais, inteiros, racionais, reais, inteiros negativos, fracionários, irracionais, imaginários, algébricos, algébricos reais e transcendentes.

Exercício 141. Assumindo a Hipótese do Contínuo (veja Capítulo 3), mostre que o conjunto dos números irracionais é equipotente a $\mathbb{R}$. Idem para o conjunto dos números transcendentes.

Mostraremos no exercício seguinte que o fato demonstrado no exercício anterior é independente da Hipótese do Contínuo. Precisamos da proposição seguinte.

Proposição 6.3.4. *Os conjuntos* $\mathbb{R} \setminus \mathbb{N}$ *e* $\mathbb{R}$ *são equipotentes.*

Demonstração. Os argumentos são similares aos utilizados nos Exercícios 129 e 61. Considere a função $f : \mathbb{R} \to \mathbb{R} \setminus \mathbb{N}$ que é a identidade em $\mathbb{R} \setminus \mathbb{Z}$, e estabelece uma bijeção entre $\mathbb{Z}$ do domínio e $\mathbb{Z}_-^*$ do contradomínio, análoga à construída no Exercício 61. Essa função é bijetora (certifique-se desse fato). □

Exercício 142. Generalizando a proposição precedente, mostre que se A é um subconjunto enumerável de um conjunto não enumerável X, então $X \setminus A$ é equipotente a X. Conclua que os conjuntos do exercício anterior são equipotentes a $\mathbb{R}$.

Exercício 143. Mostre que $\mathbb{R}$ e $\mathbb{C}$ são equipotentes.

6.4 Para além dos complexos

Uma pergunta natural, neste ponto, seria: *os conjuntos numéricos param por aí? Ou seja,* $\mathbb{C}$ *pode ser imerso propriamente em algum outro conjunto de números?* A resposta é sim! Por exemplo, $\mathbb{C}$ pode ser imerso no *anel dos quatérnios de Hamilton* (veja [9], [14]) que, no entanto, não tem mais a estrutura algébrica de corpo porque a multiplicação deixa de ser comutativa. Os quatérnios são hoje utilizados em robótica, computação gráfica e em outras áreas da ciência. Por sua vez, os quatérnios podem ser imersos nos *octônios*, no qual a multiplicação não é mais associativa. Os octônios têm importantes aplicações em ramos da física como relatividade

especial e teoria das cordas, além de se relacionarem com outras estruturas matemáticas como os chamados grupos de Lie excepcionais. Esse processo de imersão em conjuntos maiores pode prosseguir *ad infinitum* através da chamada Construção de Cayley-Dickson (veja [2]). Um resultado algébrico fundamental, devido a Frobenius (1848-1917), garante, no entanto, que as únicas *álgebras com divisão de dimensão finita sobre o corpo dos reais* são os reais, os complexos, os quatérnios e os octônios (veja [32]).

Na matemática e em suas aplicações, as estruturas de corpo ordenado completo dos reais e de corpo algebricamente fechado dos complexos são importantes por várias razões, em especial, por serem os corpos de escalares dos espaços vetoriais presentes em muitas áreas da matemática. Por outro lado, o fechamento algébrico de $\mathbb{C}$ o torna autossuficiente para abrigar as raízes de qualquer polinômio com coeficientes complexos, sobre o que há uma vasta teoria algébrica e analítica, além de serem esses os polinômios que advêm da maioria das aplicações.

Numa outra via, há o estudo abstrato de outros tipos de corpos. De um modo mais geral, o estudo de conjuntos munidos de uma ou duas operações possuindo certas propriedades é objeto da álgebra abstrata, que, na atualidade, desempenha um papel teórico e aplicado, importante também em outras áreas da ciência e em tecnologia.

Textos Universitários

A Coleção Textos Universitários destina-se a estudantes universitários cuja formação deve incluir uma sólida base matemática. Os autores são professores com reconhecida cultura nesta área e grande experiência didática.

A Sociedade Brasileira de Matemática, ao tornar disponível esta coleção, colabora de modo efetivo na tarefa de criação de uma moderna literatura científica brasileira.

ISBN 978-85-85818-45-6